ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

м. Кіровоград, 16 квітня 2015 року

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

КІРОВОГРАДСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

МЕХАНІКО-ТЕХНОЛОГІЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТУДЕНТСЬКЕ НАУКОВЕ ТОВАРИСТВО

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

“Інформаційна безпека держави, суспільства та особистості”

16 квітня 2015 року

м. Кіровоград

УДК 004.056:32.019.5
Інформаційна безпека держави, суспільства та особистості: Збірник тез доповідей Всеукраїнської науково-практичної конференції, 16 квітня 2015 року, м. Кіровоград: КНТУ, 2015. – 155 с.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Голова – **Левченко О.М.**, д-р екон. наук, проф., проректор з наукової роботи Кіровоградського національного технічного університету.

Заступник голови – **Смірнов О.А.**, д-р техн. наук, професор, завідувач кафедри програмного забезпечення Кіровоградського національного технічного університету.

Відповідальний секретар – **Мелешко Є.В.**, канд. техн. наук, доцент кафедри програмного забезпечення Кіровоградського національного технічного університету.

Члени оргкомітету:

Сидоренко В.В., д-р техн. наук, професор кафедри програмного забезпечення Кіровоградського національного технічного університету;

Стасєв Ю.В., д-р техн. наук, професор кафедри програмного забезпечення Кіровоградського національного технічного університету;

Якименко Н.М., канд. фіз.-мат. наук, доцент кафедри програмного забезпечення Кіровоградського національного технічного університету;

Петренюк В.І., канд. фіз.-мат. наук, доцент кафедри програмного забезпечення Кіровоградського національного технічного університету;

Шестерняк Н.М., керівник МОВ Кіровоградського національного технічного університету;

Кава Т.В., фахівець І категорії відділу МОВ Кіровоградського національного технічного університету;

Доренський О.П., викладач кафедри програмного забезпечення Кіровоградського національного технічного університету, науковий керівник Студентського наукового товариства Кіровоградського національного технічного університету;

Гермак В.С., викладач кафедри програмного забезпечення Кіровоградського національного технічного університету;

Константинова Л.В., викладач кафедри програмного забезпечення Кіровоградського національного технічного університету;

Даркіна В.О., голова Студентського наукового товариства Кіровоградського національного технічного університету.

Редакційна колегія: **Смірнов О.А.**, д-р техн. наук, професор (відповідальний редактор); **Мелешко Є.В.**, канд. техн. наук, доцент (відповідальний секретар); **Якименко Н.М.**, канд. фіз.-мат. наук, доцент; **Якименко М.С.**, канд. фіз.-мат. наук, доцент.

Адреса редакційної колегії: 25030, м. Кіровоград, пр. Університетський, 8, Кіровоградський національний технічний університет, тел.: (0522)390-449.

Відповідальна за випуск: Мелешко Є.В.

Збірник містить тези доповідей за матеріалами Всеукраїнської науково-практичної конференції “Інформаційна безпека держави, суспільства та особистості”, що відбулась 16 квітня 2015 року на базі кафедри програмного забезпечення Кіровоградського національного технічного університету.

ЗМІСТ

Напрямок 4.

Криптографічні засоби захисту інформації

Напрямок 5.

Стеганографічні засоби захисту інформації

Напрямок 6.

Технічні засоби захисту інформації

Напрямок 7.

Комплексні системи захисту інформації

Напрямок 8.

Захист персональних даних

Напрямок 9.

Інформаційні війни

Напрямок 10.

Електронний уряд та інші соціальні інформаційні ресурси з погляду безпеки інформації

Напрямок 1.
Інформаційна безпека держави

УДК 004.056.5:378.1 (043.2)

Синтез освіти і науки при підготовці фахівців з інформаційної безпеки в Україні

Гнатюк С.О., канд. техн. наук, доцент
Національний авіаційний університет, м. Київ

Забезпечення інформаційної безпеки (ІБ) стає все більш важливим і стратегічним питанням для окремих громадян, суспільства і держави у цілому. Як наслідок, за останні роки на ринку праці значно зріс попит на якісних фахівців у галузі ІБ – фактично, розвиток і вдосконалення системи підготовки відповідних кадрів стали одним із першочергових завдань державної політики України та інших держав. Все більша кількість вищих навчальних закладів (ВНЗ) поступово перекваліфіковуються на підготовку кадрів у галузі ІБ. У зв'язку з цим ВНЗ, які готують фахівців у галузі ІБ, стикаються з цілою низкою проблем від оперативності та якості вирішення яких залежить затребуваність підготовлених кадрів на ринку праці і, як наслідок, рейтинг самого ВНЗ. Відповідно до сучасних світових тенденцій такими проблемами є:

1. Законодавство держави в галузі ІБ повинне враховувати міжнародний досвід, базуватися на основних стандартах і кращих світових практиках у сфері ІБ, кібербезпеки та захисту критичної інформаційної інфраструктури.
2. Система підготовки кадрів в галузі ІБ повинна бути чітко структурованою: окрема галузь знань повинна систематизувати всі бакалаврські напрями і відповідні їм магістерські програми.
3. Крім освітніх, повинні обов'язково бути затверджені й наукові спеціальності, які охоплюють усі без виключень актуальні напрями наукових досліджень в галузі ІБ і узгоджені з відповідними аналогами провідних світових держав.
4. Мережа спеціалізованих вчених рад повинна об'єднувати провідних учених держави у галузі ІБ з можливістю залучення відомих закордонних фахівців (у якості, співконсультантів, опонентів, членів рад) з метою якісної експертизи дисертаційних робіт.
5. Спеціалізовані наукові видання (журнали та збірники наукових праць) і періодичні наукові загальнодержавні та міжнародні конференції (семінари, конгреси, симпозіуми тощо) повинні забезпечувати якісне висвітлення та апробацію наукових і практичних результатів перед світовою громадськістю.
6. При профільних ВНЗ повинні функціонувати спеціалізовані лабораторії для реалізації державних замовлень щодо розробки та сертифікації власних комплексних систем захисту інформації з обов'язковим залученням докторантів, аспірантів і студентів випускаючих кафедр.
7. Повинні бути розроблені відповідні програми та при профільних ВНЗ мають функціонувати центри підвищення кваліфікації в галузі ІБ.
8. Навчальні програми та плани повинні своєчасно і безперервно удосконалюватися відповідно до тенденцій розвитку інформаційних та комунікаційних технологій.
9. Держава повинна підтримувати наукові дослідження щодо питань забезпечення ІБ, а самі питання мають бути включені в пріоритетні національні напрямки науки і техніки – це

сприятиме розробці вітчизняних апаратних та програмних засобів для захисту критичних інформаційних ресурсів держави.

Таким чином, лише інтеграція освіти і науки за підтримки держави дозволить ВНЗ готувати висококласних конкурентоспроможних на світовому ринку спеціалістів у галузі ІБ, які будуть затребувані у всіх галузях народного господарства, як в рамках держави, так і за її межами.

УДК 004.056.5

Основні цілі та об’єкти інформаційної безпеки держави

Притула А.В., студент 2 курсу
Науковий керівник – Константинова Л.В., викладач
Кіровоградський національний технічний університет, м. Кіровоград

Для дослідження явища інформаційної безпеки треба розумітись у певних термінах та значеннях. Отже, для того щоб успішно орієнтуватись в інформаційній безпеці держави, в першу чергу треба розібратись у понятійному апараті.

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення (у цьому значенні частіше використовують термін "захист інформації") [1, 2].

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Інформаційна безпека держави – це стан її захищеності, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам [2].

Основні способи посягань на інформаційну безпеку держави [2, 4]:

Спеціальні інформаційні операції (СІО) – це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію, які передбачають вплив на її свідомість і поведінку за допомогою використання організованої інформації та інформаційних технологій для досягнення певної мети.

Акти зовнішньої інформаційної агресії (АЗА) – легальні та (або) протиправні акції, реалізація яких може мати негативний вплив на безпеку інформаційного простору держави.

Інформаційний тероризм (ІТ) – небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади та управління, пов’язані з поширенням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також викривлення об’єктивної інформації, що спричиняє виникнення кризових ситуацій у державі, нагнітання страху і напруги в суспільстві.

Комп’ютерна злочинність – протиправні діяння у сфері використання електронних обчислювальних машин (комп’ютерів), автоматизованих систем та комп’ютерних мереж, за які чинним Кримінальним кодексом (КК) України передбачено відповідальність.

Об’єктами забезпечення інформаційної безпеки держави є [2]:

1. Інформаційно-телекомунікаційна інфраструктура (суб’єкти та засоби створення, поширення інформації і передачі даних);
2. Інформація (особиста, конфіденційна, власність держави, з обмеженим доступом);
3. Свідомість (особи, групи, суспільства).

Для протидії посяганню на інформаційну безпеку держави слід виконувати наступні завдання:

1. Забезпечення інформаційної безпеки усіх складових елементів системи управління НБ;
2. Забезпечення інформаційно-аналітичного потенціалу країни;
3. Реалізація державної політики інформаційної безпеки в рамках реалізації політики національної безпеки;
4. Ведення активної розвідувальної, контррозвідувальної і оперативно-розшукової діяльності з метою забезпечення інформаційної безпеки через здобуття необхідної інформації для відпрацювання стратегічних, тактичних і оперативних рішень у сфері управління інформаційною безпекою та вироблення механізмів їх реалізації;
5. Виявлення, попередження і припинення розвідувальної та іншої, спрямованої на нанесення шкоди інформаційній безпеці України, діяльності спеціальних служб, а також окремих осіб чи організацій;
6. Виявлення, попередження і припинення інформаційного тероризму та іншої діяльності, спрямованої на підрив функціонування системи управління НБ;
7. Моніторинг (спостереження, оцінка та прогноз) стану інформаційної безпеки у зв'язку із впливом загроз та небезпек як зсередини, так і ззовні системи управління НБ;
8. Протидія технічному проникненню до інформаційних систем об'єктів інформаційної безпеки з метою вчинення злочинів, проведення диверсійно-терористичної та розвідувальної діяльності;
9. Запобігання можливої протиправної та іншої негативної діяльності суб'єктів системи забезпечення національної безпеки зсередини системи їй на шкоду;
10. Забезпечення збереження державної таємниці;
11. Організація демократичного цивільного контролю за функціонуванням системи управління НБ тощо.

Згідно з Законом України «Про основи національної безпеки України» [3] основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері є:

1. Прояви обмеження свободи слова та доступу до публічної інформації;
2. Поширення засобами масової інформації культу насильства, жорстокості, порнографії;
3. Комп'ютерна злочинність та комп'ютерний тероризм;
4. Розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави;
5. Намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Отже, для збереження інформаційної безпеки держави слід застосовувати правові норми, які записані в Конституції України. Також для інформаційної безпеки держави слід дотримуватись наступних правил, до яких входить [4]:

1. Забезпечення функціонування ефективно діючої комплексної системи захисту інформаційних ресурсів системи управління НБ;
2. Забезпечення захисту системи управління НБ від хибної, спотвореної та недостовірної інформації;
3. Забезпечення розробки та застосування правових, організаційних і економічних механізмів стосовно форм та засобів обігу інформаційних ресурсів України (ринку інформації, інформаційних технологій, засобів обробки інформації та інформаційних послуг);
4. Регулювання інформаційного співробітництва, спрямованого на забезпечення рівноправного і взаємовигідного використання національних інформаційних ресурсів у

процесі міжнародного обміну.

5. Здійснення єдиної державної політики наукової підтримки системи управління формуванням, розвитком і використанням національних інформаційних ресурсів.

Список літератури:

1. Інформаційна безпека [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Інформаційна_безпека

2. Петрик Валентин Сутність інформаційної безпеки особи і держави [Електронний ресурс]. – Режим доступу: http://www.justinian.com.ua/article.php?id=3222

3. Закон України «Про основи національної безпеки України» //Відомості Верховної Ради України. – 2003. – № 39. – Ст. – 351. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/964-15

4. Ліпкан В.А. Національна безпека України – навч. посіб. / В.А. Ліпкан. – К.: Кондор, 2008. – 552 с.

УДК 32.001: 004.056 (477)

Механизмы информационной безопасности Украины

Семченко О.Р., канд. полит. наук

Одесская национальная академия связи им. А.С. Попова, г. Одесса

В последнее время в политическом лексиконе появилось понятие «гибридная война», сочетающая разные направления: военное, экономическое, политическое, идеологическое и др. Однако наибольшее значение в ходе военного противостояния все чаще играет именно информационная составляющая.

В условиях российской агрессии особо отчетливо проявилось, что Украина нуждается в информационных механизмах, способных защитить ее информационные ресурсы, противодействовать враждебному внешнему влиянию на общественное мнение украинцев. Неслучайно, многие эксперты полагают, что одной из причин событий на Донбассе стало информационное отсутствие Украины в информационном пространстве своей восточной части. Манипуляции массовым сознанием жителей Донбасса со стороны российских СМИ привели к враждебному отношению жителей этого региона к центральной украинской власти.

Таким образом, проблема защиты информационного пространства Украины приобретает сегодня особую актуальность. Закономерно, что Министерство информационной политики считает одной из своих важных задач - создать концепцию информационной безопасности Украины. В течение 2015 года Министерство собирается создать канал иновещания, а также интернет-платформу для донесения оперативной информации об Украине.

В политическом и экспертном сообществах нет единодушия относительно содержания механизмов, с помощью которого защита информационного пространства возможна. Одни считают, что во время военных действий, которые, фактически, имеют место в Украине, должна быть введена цензура на информацию, другие считают, что это будет противоречить демократическим устремлениям Украины, и не будет поддержано демократической международной общественностью. Очевидно, что, как всегда, истина где-то посередине. В условиях военного конфликта каждое неосторожное слово может использоваться противником в своих пропагандистских целях. Так, мы помним октябрьский демарш Национальной гвардии в защиту прав военнослужащих, который, как оказалось, был организован российскими спецслужбами. Данное информационное наступление было проведено по всем правилам информационной войны. А именно, были использованы

сложности украинской ситуации, возникшей в связи с российской агрессией. Если проанализировать информационный контент того периода, то мы обнаружим, что в СМИ преобладала информация негативного характера, официальная информация создавала впечатление недосказанности, а значит, мало вызывала доверия у зрителей. Это в свою очередь провоцировало зрителей на поиск альтернативной информации, в первую очередь, в Интернете. Все это привело к снижению уровня устойчивости населения перед дезинформацией и повышению уровня протестности.

Информационные механизмы политической стабильности необходимы для того, чтобы минимизировать последствия информационной войны, объектом которой может быть Украина. Как известно, против Украины такую войну в настоящее время развернуло российское государство.

Информационная война, это:

- совокупность политико-правовых, социально-экономических и др. действий, направленных на захват информационного пространства;

- вытеснение противника из информационной сферы, разрушение его коммуникаций, лишение средств передачи сообщений и др. [1, с. 256]. По мнению известного теоретика информационной войны С.П. Расторгуева, «информационная война между двумя информационными системами - это открытые и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере» [2, с. 58].

Таким образом, Украина, как никогда, нуждается в самых современных формах противодействия информационной агрессии. Однако, субъекты государственной информационной политики ограничиваются запретами на вещание российскими каналами, российские сериалы и т.д. На наш взгляд, такие меры противоречат демократическим нормам и мало способствуют заявленному предназначению - защитить украинское информационное пространство.

25 января 2015 г. председатель парламентского комитета по вопросам информации и свободы слова Виктория Сюмар написала в Facebook, что сделает все возможное, чтобы уже завтра запретить российские информационные продукты и ввести санкции по отношению к РФ, в том числе и касательно права собственности на СМИ, работающие в Украине [3]. Таким образом, некоторые политики и эксперты подталкивают власть к введению тотальной цензуры в СМИ, в Интернете, в почтовых сообщениях и пр. К тому, чтобы ограничить число СМИ, аккредитованных в Украине.

Уменьшат ли такие меры поток лжи и дезинформации в украинском информационном пространстве? Думается, что нет. Если, конечно же, кто-нибудь не предложит отключить в Украине Интернет.

Подобные механизмы борьбы с субъектами угроз политической стабильности характерны для стран Ближнего Востока и СНГ, в которых наряду с органами и силами государственной и общественной безопасности важную роль играет контроль над информационной сферой государства, включающий надзор и цензурирование средств массовой информации, ресурсов сети Интернет, контроль над блогосферой и сообщениями электронной почты [4, с. 39].

Учитывая, что информационная политика авторитарной власти и демократической власти кардинально отличается, думается, что информационная политика Украины должна принципиально отличаться от информационной политики, например, России и Беларуси, основанной на тотальной информационной цензуре. И, конечно же, она должна отличаться от информационной политики предыдущей власти.

Известный эксперт Андреас Умланд справедливо отмечает, что Украина в своей информационной политике не должна уподобляться России, манипулируя фактами и дезинформацией: «Доказанное манипулирование фактами сравняет Украину и Россию в глазах международной общественности». Иначе, Украина может утратить доверие демократических стран. Однако противодействовать российской пропаганде, как внутри

страны, так и за рубежом, необходимо. И здесь возникает вопрос, как противодействовать, не применяя методы России? Следует признать, что в украинских СМИ иногда мелькает информация, не соответствующая действительности. Не всегда это преднамеренно, бывают и ошибки. Однако такие ошибки ведут к ухудшению имиджа Украины в глазах зарубежной общественности и прессы, которые получат, таким образом, повод говорить о ведении информационной войны обеими сторонами.

По мнению Андреаса Умланда, необходимо регулярно разоблачать дезинформацию российских СМИ по схеме StopFake. Это поможет зарубежной общественности лучше понимать то, что происходит в Украине. Не секрет, что российская пропагандистская машина все прошедшие годы мощно работала в европейских странах. А Украина наоборот, проигрывала в борьбе за зарубежное общественное мнение. Результаты не заставили себя ждать. Население в европейских странах не все, происходящее в Украине, понимает в полной мере.

В последнее время в зарубежной прессе буквально каждый день появляются статьи, посвященные Украине. Однако, рост знаний об Украине за ее пределами происходит в основном благодаря гражданскому обществу, а не государству [5].

Было бы разумно, если бы Украина, избравшая демократический европейский путь развития, сумела удержаться в рамках демократических ценностей и норм и воздержаться от неоправданных запретов на информацию для своих граждан. Это очень важно для имиджа Украины за рубежом. Чтобы демократические страны не могли упрекнуть Украину в том, что ее информационная политика ничем не отличается от российской.

Список литературы

1. Политические коммуникации: / [Петрунин Ю.Ю. и др]; - под. ред. А.И. Соловьева. – М.: Аспект Пресс, 2004. – 332 с.

2. Расторгуев С.П. Информационная война / С.П. Расторгуев. – М.: Радио и связь, 1999. – 416 с.

3. Сюмар хочет запретить российские СМИ на Украине "уже завтра" [Электронный ресурс]. – Режим доступа: http://ria.ru/world/20150125/1044214745.html

4. Семченков А.С. Противодействие современным угрозам политической стабильности в системе обеспечения национальной безопасности России : автореф. дис… д. політ. н. : спец. 23.00.02 – Политические институты, процессы и технологии / Андрей Сергеевич Семченков. – М., 2012. – 50 с.

5. Андреас Умланд: Ложь не поможет ни Киеву, ни Москве [Электронный ресурс]. – Режим доступа: http://www.stopfake.org/andreas-umland-lozh-ne-pomozhet-ni-kievu-ni-moskve/

УДК 004.413:004.056.5

Огляд застосування математичного апарату до інформаційної безпеки України

Якименко Н.М., канд. фіз.-мат. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Внаслідок бурхливого розвитку інформаційних технологій основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси. Відбувається перерозподіл реальної влади від традиційних структур до центрів управління інформаційними потоками, зростає впливовість засобів масової інформації (ЗМІ). Інформатизація та комп’ютеризація докорінно змінюють обличчя суспільства. За таких обставин забезпечення інформаційної безпеки поступово виходить на перший план у проблематиці національної безпеки.

Інформаційна безпека (Information Security) має три основні складові: конфіденційність, цілісність і доступність. Конфіденційність належить до захисту чутливої інформації від несанкціонованого доступу. Цілісність означає захист точності і повноти інформації і програмного забезпечення. Доступність – це забезпечення доступності інформації і основних послуг для користувача в потрібний для нього час [1].

Зі зростанням науково-технічного прогресу зростає і важливість питання інформаційної безпеки громадянина, суспільства, держави. Тобто інформація стала чинником, який може призвести до значних технологічних аварій, військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів, і чим вищий рівень інтелектуалізації та інформатизації суспільства, тим потрібнішою стає надійна інформаційна безпека, оскільки реалізація інтересів, людей та держав все більше здійснюється за допомогою інформатизації. Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд та мораль як окремих осіб, так і суспільства в цілому, нав’язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах [2].

Завдання інформаційної безпеки - створення системи протидії інформаційним загрозам [4] та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. При виникненні криз, загостренні конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї.

Головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав’язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку. Власне, це є загрозою суверенітету України в життєво важливих сферах суспільної й державної діяльності, що реалізовується на інформаційному рівні. Стратегічне інформаційне протистояння є самостійним і принципово новим видом протистояння, здатним вирішувати конфлікт без застосування збройних сил у традиційному розумінні.

Для вивчення закономірностей інформаційного протистояння та аналізу його кількісних характеристик необхідно формалізувати як поняття рівня інформаційної озброєності держави, так і механізм еволюції ресурсного потенціалу конкретної держави та вплив зовнішнього оточення. В даному випадку за основу аналізу вибраний інформаційний стан України. Як базову розглядають модель вирішення інформаційного конфлікту двох країн, яка складена на основі моделі Річардсона - Каспарова [5]. Дослідивши математичну модель [6], одержано висновок: кожна держава, що є частиною світового інформаційного простору, має виробити комплекс заходів для власного сталого інформаційного розвитку в умовах жорсткої конкуренції з урахуванням чинників інформаційної безпеки.

Аналіз сучасних літературних джерел [7, 11–13] свідчить про обмеженість наукової та методичної бази, яку можна використати для кількісного та якісного оцінювання стану охорони державної таємниці. Це особливо важливо тоді, коли відсутня повна інформація про існуючий стан, а вихідні дані, що підлягають вивченню (експертизі), задані нечітко (розмито) і часто ґрунтуються на судженнях та інтуїції експерта (людський фактор) [11, 12]. Тому для роботи з нечіткими детермінованими величинами, як правило, застосовують математичний апарат теорії нечітких множин [8]. Відомо [1, 3], що для експертизи використовуються “Звід відомостей, що становлять державну таємницю”(ЗВДТ) [12] та Перелік службової інформації як акти, у яких у вигляді статей з коротким описом їх змісту із визначеним ступенем обмеження доступу зведено відомості, що становлять державну таємницю і службову інформацію. Відповідно матеріальним носіям інформації, що містять такі відомості, надається гриф секретності “таємно”, “цілком таємно” і “особливої важливості” або гриф

“для службового користування”. З наведених у [11–13] даних “Звід відомостей, що становлять державну таємницю” та Перелік службової інформації можуть бути представлені як складна орієнтована інформаційна мережа (СОІМ) з наявною онтологічною ієрархією з можливостями визначення цінності (важливості) інформації. Отже, для розроблення методу нечіткої класифікації відомостей, що становлять державну таємницю за визначеними критеріями, застосовують теорію нечітких множин [4, 9, 10], а також СОІМ ЗВДТ [11–13].

Управління інформаційними ризиками є одним з найбільш актуальних напрямків стратегічного і оперативного менеджменту в галузі інформаційної безпеки. При аналізі та оцінці ризиків традиційно використовуються математичні методи підтримки прийняття рішень: табличний метод, метод аналізу ієрархій, метод експертних оцінок.

Провідна роль у забезпеченні інформаційної безпеки в інформаційно-телекомунікаційних системах відводиться криптографії, одними із головних задач є: забезпечення конфіденційності, цілісність та автентичність даних, що передаються [14, с.5]. Криптографія – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації сторонніми) і автентичності (цілісності і справжності автора) інформації. На сьогодні криптографія, як галузь знань, та криптографічний захист інформації, як окрема галузь діяльності, стосується: питань шифрувальної справи, новітніх технологій електронної торгівлі, систем автоматизованого управління, звітування та контролю тощо.

Таким чином, математичний апарат необхідний для ефективного управління інформаційною безпекою держави Україна.

Список літератури

1. Близнюк І.М. Інформаційна безпека України та заходи її забезпечення / І.М. Близнюк // Науковий вісник Національної академії внутрішніх справ України. – 2008. – № 5. – С. 206-214.

2. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О.М. Горбатюк // Вісник Київського університету імені Т.Шевченка. – 2009. – Вип. 14: Міжнародні відносини. – С. 46-48.

3. Сороківська О.А., Гевко В.Л. Інформаційна безпека підприємства: нові загрози та перспективи // Вісник Хмельницького національного університету. – 2010. - № 2, Т. 2. - С. 32-35

4. Бондаренко В., Литвиненко О. Інформаційна безпека сучасної держави: концептуальні роздуми / В. Бондаренко, О. Литвиненко [Електронний ресурс] Режим доступу: http://www.crime-research.iatp.org.ua/ library/strateg.htm.

5. Саати Т. Л. Математические модели конфликтных ситуаций. - М. : “Сов. Радио”, 1977. - 304 с.

6. Боднар І. Р. Інформаційна безпека як основа національної безпеки // Механізм регулювання економіки. - Суми. – 2014

7. Архипов О.Є. Оцінювання ефективності системи охорони державної таємниці: монографія /О.Є. Архипов, І.Т. Бородавко, В.П. Ворожко. – К.: Наук.-вид. відділ НА СБ України, 2007. – 63 с.

8. Дрейс Ю.О. Визначення рівня компетентності експертів експертної комісії з питань державної таємниці / Ю.О. Дрейс, О.Г. Корченко // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. – Житомир: ЖВІ НАУ, 2011. – Вип. 4. – С. 190–196.

9. Архипов О.Є. Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою: монографія / О.Є. Архипов, О.Є. Муратов. – К.: Наук.-вид. відділ НА СБ України, 2011. – 195 с.

10. Дрейс Ю.О. Розрахунок коефіцієнтів захищеності відомостей, що становлять державну таємницю / Ю.О. Дрейс, Н.С. Вишневська, Ю.Є. Хохлачова // Захист інформації. – Вип. №3 (48). – 2010. – С.10–14.

11. Корченко О.Г. Нечітке моделювання лінгвістичної змінної “інформація” за змістом відомостей та видом операцій, що виконуються над нею / О.Г. Корченко, Ю.О. Дрейс // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем: зб. наук. праць. – Житомир: ЖВІ НАУ, 2009. – Вип.2 – С.102–108.

12. Корченко О.Г. Нечітке моделювання вхідної інформації АРМ державного експерта з питань таємниць / О.Г. Корченко, Ю.О. Дрейс // “Актуальні проблеми забезпечення інформаційної безпеки держави”: збірник матеріалів наук.-практ. конф., 20 березня 2009. – К.: ІЗІзОД НА СБ України, 2009. – С.190-191.

13. Архипов О.Є. Застосування онтологічної ієрархії у задачах визначення цінності інформації / О.Є. Архипов, М.А. Петренко // Захист інформації. – Вип. №1(54). – 2012. – С.45-52.

14. Бевз О.М. Шифрування даних на основі високонелінійних булевих функцій та кодів з максимальною відстанню : монографія \ О.М. Бевз, Р.Н. Квєтний – Вінниця:ВНТУ, 2010. – 96 с.

Напрямок 2.
Захист інформації в комп'ютерних системах та мережах

УДК 004.056.55(043.2)

Таксономія та застосування алгоритмів, натхнених внутрішніми біологічними схемами

Ануфрієнко К.П., канд. техн. наук,
Коваленко Ю.Б., канд. пед. наук, доцент,
Березін І.С., студент 2 курсу,
Щудлик І.А., студент 2 курсу
Національний авіаційний університет, м. Київ

У порівнянні з традиційними мережевими механізмами управління, самоорганізація є перспективним підходом для виконання поточних (і майбутніх) вимог проектування мереж. Схеми з біологічних явищ є підходящими кандидатами для управління самоорганізацією мережі, так як вони, як правило, використовують прості і іноді навіть ідентичні робочі набори правил для керівництва кожним об'єктом, щоб виконати місцеві спостереження, і взаємодії з іншими, щоб спільно виробляти ефективні та дієві оперативні моделі в досягненні цілей всієї групи. Для класифікації біологічно натхнених алгоритмів розроблено три головних категорії біологічно надихаючих явищ: алгоритми, натхненні внутрішніми біологічними системами; алгоритми, натхненні однорідними біологічними організмами; алгоритми, натхненні гетерогенними біологічними організмами.

Алгоритми, натхненні внутрішніми біологічними схемами (ВБС), є схемами внутрішнього розвитку, підтримки та реакції у організмах. В основному, різні компоненти організмів співпрацюють з метою досягнення кількох біологічних цілей. Взаємодія зазвичай складається з взаємодій між внутрішніми компонентами, а також взаємодії між внутрішніми компонентами і зовнішніми середовищами. Класифікація цих алгоритмів наведена на рисунку 1.

Ці біологічно натхнені алгоритми можуть бути застосовані до мережевої будови безпосередньо. Для процедури в кожному алгоритмі зазвичай немає універсально визначеної математичної моделі. Правила дій для компонентів в мережевій системі розроблені на основі поведінки відповідних компонентів в біологічних системах. У таблиці 1 підсумовано сфери застосування, які придатні для використання ВБС до комп'ютерних мереж.

Штучні імунні системи (ШІС) натхненні імунною системою хребетних тварин, виявляють зміни в навколишньому середовищі або захищаються від ненормальної поведінки в комп'ютерній системі. Імунна система хребетних (ІСХ) має багаторівневий захист і проти патогенів, які є як чужорідними, так і потенційно шкідливими білками. Цей захист включає в себе таке: фізичні бар'єри, наприклад, шкіри, хутра, і виділення, для запобігання входу патогенів у організм; вроджену імунну систему, яка використовує лейкоцити для неспецифічного знищення або поглинання вторгнення патогенних мікроорганізмів і потенційно небезпечних клітин; адаптивну імунну систему для швидкого реагування на патогени, що зустрічалися раніше з використанням лімфоцитів, таких як В-клітини і Т-клітини. Є три модельні представлення ІСХ, що застосовується більшістю ШІС: гуморальна імунна реакція (В-клітинна активність), клітинний імунітет (Т-клітинна активність), і теорія

небезпеки.

В *гуморальній імунній реакції,* В-клітини ідентифікують патогени антигеном, які вони виробляють в імунній фазі. Виходячи з цього, вони знищують патогенні мікроорганізми, а потім секретують антитіла, які залишаються всередині організму протягом відносно тривалого періоду, які відразу ж реагують на патогени з тим же типом антигену. Довгу пам'ять і властивості самонавчання цього механізму адаптовані ШІС в розробці системи виявлення атак (СВА).

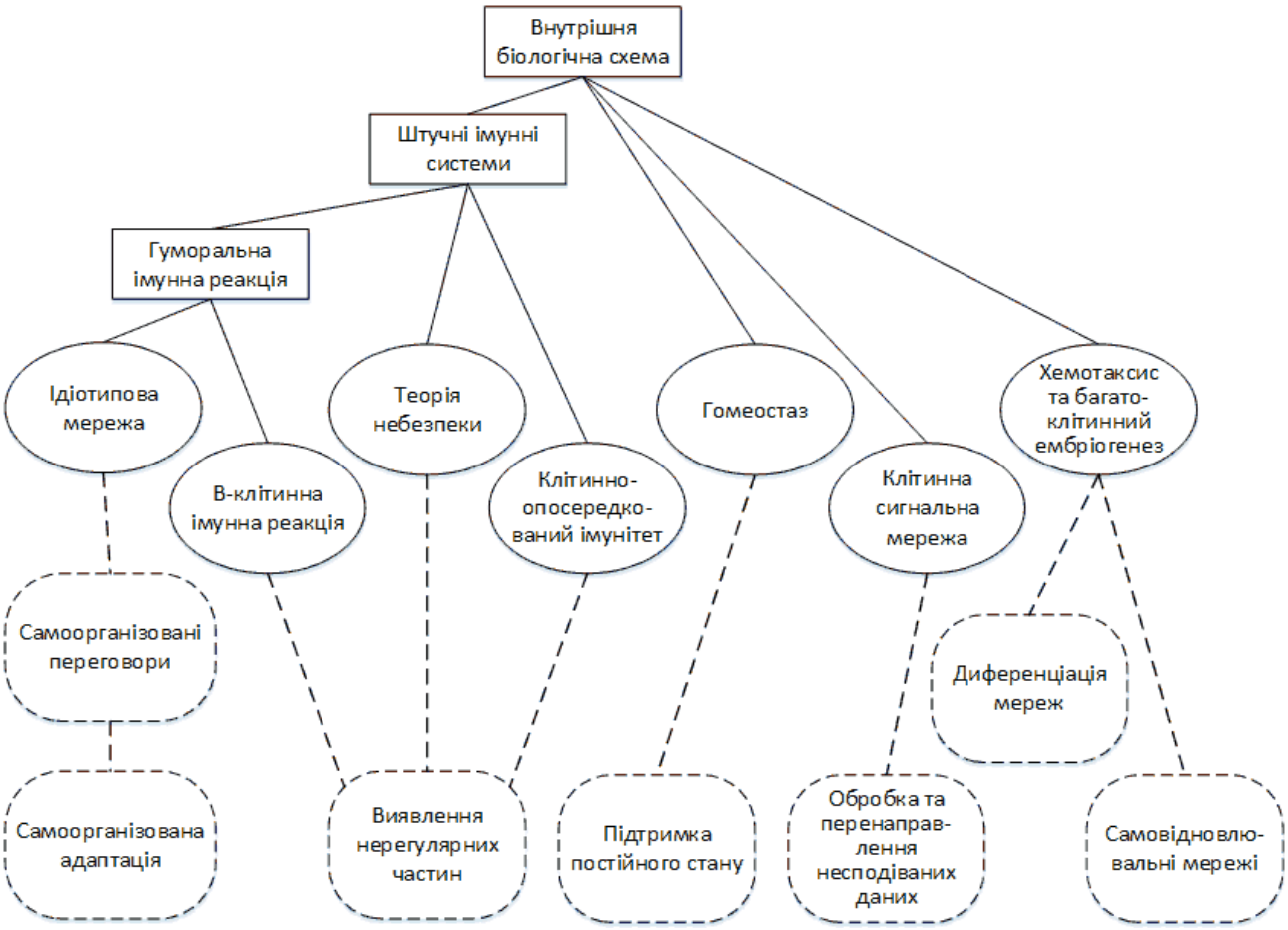

Рисунок 1 – Таксономія алгоритмів, натхнених внутрішніми біологічними схемами, з їх застосуванням

Таблиця 1 – ВБС та їх застосування у комп’ютерних мережах

ВБС	**Сфера застосування**
В-клітинна імунна реакція	Виявлення чужорідних об’єктів або об’єктів, що неправильно себе поводять
Клітинно-опосередкований імунітет	
Теорія небезпеки	
Ідіотипова мережа	Самоорганізовані переговори про конфігурацію або компоненти
Гомеостаз	Підтримка постійного стану системи
Клітинна сигнальна мережа	Обробка та перенаправлення несподіваних даних
Хемотаксис та багатоклітинний ембріогенез	Диференціація мережевої структури або функціональностей; самовідновлювальні мережі

В *клітинному імунітеті,* Т-клітини зв'язують і вбивають заражені або потенційно шкідливі клітини. Тим не менш, через псевдо-випадкову генерацію Т-клітин особливості

поверхні використовуються для зв'язування клітин-мішеней, деякі Т-клітини можуть також руйнувати здорові клітини. Щоб запобігти цьому побічному ефекту, Т-клітини негативно обираються перед входом в кровообіг, тобто, всі Т-клітини, чиї функції поверхні будуть зв'язуватися з здоровими клітинами, руйнуються. Випадкова варіація і негативні схеми відбору адаптовані ШІС в дизайні виявлення вторгнень.

Теорія небезпеки стверджує, що, коли клітини гинуть від патогенних мікроорганізмів, вони випромінюють набір сигналів. Імунна система потім може визнати існування і характеристики патогенів після отримання цих сигналів небезпеки. Неефективно, навіть неможливо відобразити весь чужорідний всесвіт безліччю детекторів, особливо, коли однорідний і чужорідний набір систем будуть змінюватися з плином часу. В результаті помилкові спрацьовування по виявленню патогенних мікроорганізмів виявляються в негативній процедурі відбору. Теорія небезпеки може бути застосована в ШІС для подолання цього недоліку негативної схеми відбору.

Властивість біологічних систем підтримувати свій власний стабільний статус, реагуючи на безперервні зміни в їх внутрішніх і зовнішніх умовах відома як гомеостаз. Цей вид явищ можна спостерігати в таких механізмах, як регулювання температури тіла або підтримка артеріального тиску.

Дослідницькі зусилля були поміщені на модельне представлення гомеостазу в нервову, ендокринну та імунну системи. Хоча повсюдно застосовуються математичні моделі або алгоритми для гомеостазу вже визначені, Ніл та ін. запропонували модель гомеостазу, досягнуту співробітництвом між штучною ендокринною системою (AES) і штучними нейронними мережами (ANN). В їх моделі, різні види клітинних залоз виділяють відповідні гормони при реагуванні на зовнішні подразники. Концентрація виробництва гормонів буде змінюватися в залежності від геометричної розпаду.

Клітинна сигнальна мережа

На молекулярному рівні клітини спілкуються одна з одною за допомогою процесу, названого сигнальним шляхом. В одному механізмі рецептори, розташовані на поверхні клітини, можуть пов'язувати молекули, пов'язані з зовнішньою клітиною. Пов'язані молекули активують сигнальні молекули всередині клітини, що може, в свою чергу, активувати далі вниз за течією сигнальних молекул, внаслідок чого виходить ефект доміно білок-білок. З іншого боку, молекули з віддалених клітин, що проходять через кровоносну систему, можуть бути пов'язані з рецепторами в клітині.

З глобальної точки зору, кожна окрема клітина виконує прості, але конкретні відповіді на інформаційні молекули, які залежать від типу сигналу і стану клітини, що призводить до самоорганізації, виникає узгоджена поведінка системи в механізмі. Ця виникаюча властивість корисна для застосування в управлінні великими розподіленими системами. Хоча це явище не було математично модельовано, існує два основних застосування цієї ідеї: заснована на правилах сенсорна мережа; метаболічний підхід до стійкості комунікаційного протоколу.

Хемотаксис та багатоклітинний ембріогенез

Феномен хемотаксиса, в якому клітини переміщаються відповідно градієнту хімічних речовин у навколишньому середовищі, і ті, що спостерігаються в багатоклітинному ембріогенезі, тобто морфогенезі, пропонує біологічні примітиви для самоорганізації в технічних системах.

Отже, існує кілька різних біологічно натхнених алгоритмів, що натхненні метафорою ІСХ і націлені на одну мету — виявлення чужорідностей в мережевих системах, що, безумовно, має значення для забезпечення безпеки комп’ютерних мереж.

УДК 004.056.55

Сучасні системи виявлення атак

Бісюк В.А., викладач
Кіровоградський національний технічний університет, м. Кіровоград

Розвиток сучасних інформаційних систем обумовлений досягненнями телекомунікаційних та мережних технологій, що використовуються для розподіленої обробки інформації. Відповідно виникають нові види атак на інформаційні системи (ІС), з багаторівневими алгоритмами та розподіленим характером [1].

Кожен рік спостерігається збільшення кількості нових видів атакуючих впливів та постійний зріст загальної кількості атак на ІС, як в державних так і в комерційних структурах. Це обумовлює необхідність розробки і впровадження більш гнучких засобів виявлення та запобігання атакам в якості допоміжних засобів захисту інформації. До таких засобів відносять системи виявлення атак (СВА) [2].

Сучасна СВА (рис. 1) повинна виконувати розподілений збір та інтелектуальний аналіз інформації з декількох джерел ІС, а також мати здатність виявляти та запобігати появі нових видів атак.

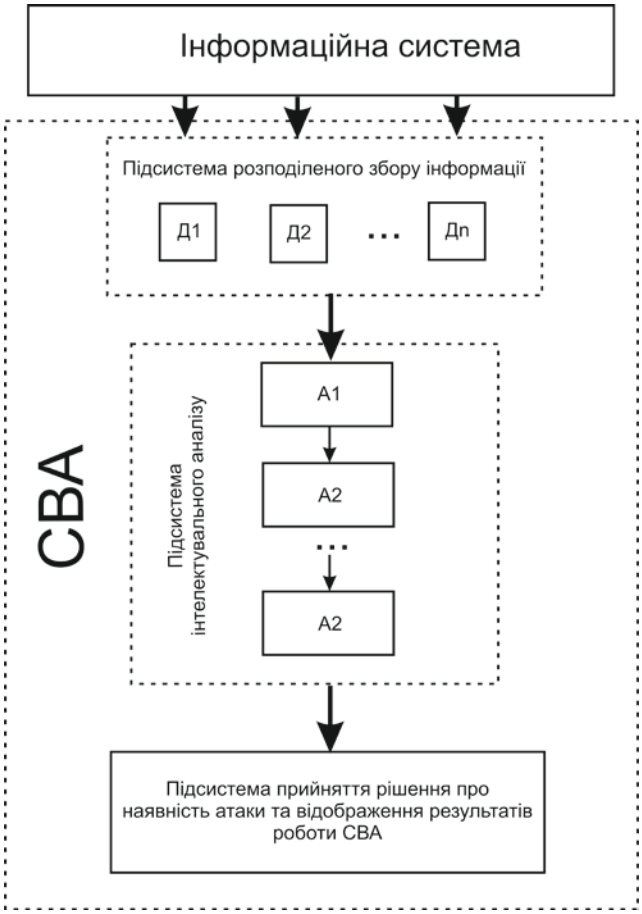

Рисунок 1 – Структура СВА з розподіленим збором та інтелектуальним аналізом інформації, де:

- Д1, Д2, Дn – розподілені датчики збору інформації;
- А1, А2, Аn – інтелектуальні адаптивні аналізатори.

Для розподіленого збору і аналізу інформації сучасні СВА оснащують набором

автономних інформаційних датчиків, які ще називають інформаційними агентами, а таку СВА називають «багатоагентною» [3]. Кількість і типи датчиків залежать від особливостей конкретної ІС. Відповідно до загальної структури ІС виділяють такі типи датчиків:

- датчики програмного забезпечення;
- датчики хосту (передають інформацію про функціонування окремої робочої станції ІС);
- датчики мережі (інформація про внутрішньомережевий трафік);
- міжмережеві датчики (передають інформацію про обмін даними між мережами).

Вся накопичена інформація передається підсистемі інтелектуального аналізу, яка містить один або декілька модулів аналізаторів, які виконують аналіз отриманої інформації і передають результати своєї роботи наступному аналізатору або підсистемі прийняття рішення про наявність атаки. Для того, щоб виявляти нові типи атак, аналізатори СВА будують на основі адаптивних алгоритмів.

Список літератури

1. Abraham A. and Thomas J., Distributed Intrusion Detection Systems: A Computational Intelligence Approach. // Applications of Information Systems to Homeland Security and Defense, Abbass H.A. and Essam D. (Eds.), Idea Group Inc. Publishers, USA, 2005

2. Смелянский PJL, Гамаюнов Д.Ю. Современные некоммерческие средства обнаружения атак // Факультет Вычислительной Математики и Кибернетики, МГУ им. М. В. Ломоносова, Москва, 2002 г.

3. Тарасов В.Б. От многоагентных систем к интеллектуальным организациям: философия, психология, информатика. М.: Эдиториал УРСС, 2002. - 352 с.

УДК 004.738.2

Дослідження принципів роботи технологій VPN

Богатиренко А.С., студентка 5 курсу
Науковий керівник – Якименко Н.М., канд. фіз.-мат. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Мережа Інтернет побудована на принципі відкритих систем. Інформація передається по загальнодоступним каналам, тому можливе порушення конфіденційності та цілісності інформації. Концепція побудови віртуальних приватних мереж VPN активно розвивається для ефективної протидії мережним атакам та для забезпечення можливості безпечного використання відкритих мереж. Віртуальною приватною мережею VPN (Virtual Private Network) називають об’єднання локальних мереж та окремих комп’ютерів через відкрите зовнішнє середовище передачі інформації в єдину віртуальну приватну мережу, яка забезпечує безпеку даних.

VPN формується шляхом побудови віртуальних захищених каналів зв'язку, створюваних на базі відкритих каналів зв'язку загальнодоступної мережі. Ці віртуальні захищені канали зв'язку називаються тунелями VPN. Мережа VPN дозволяє за допомогою тунелів VPN безпечно передавати інформацію через Інтернет.

Мережа VPN може бути організована як за допомогою програмного, так і за допомогою апаратного забезпечення. Організація VPN мережі з програмним рішенням передбачає програмне забезпечення, що встановлюється на підключеному до мережі комп'ютері, який забезпечує функціональність VPN. Програмно-апаратне забезпечення VPN мережі реалізується за допомогою комплексу програмно-апаратних засобів. Така реалізація забезпечує продуктивність і захищеність.

Найпоширеніший метод створення тунелів VPN − інкапсуляція. Тунелювання (tunneling) або інкапсуляція (encapsulation) − спосіб передачі інформації через проміжну мережу. При інкапсуляції інформація не передається в згенерованому вузлом-відправником

вигляді, а забезпечується додатковим заголовком і містить інформацію про маршрут, що дозволяє інкапсульованим даним проходити через проміжну мережу Інтернет. На кінці тунелю інформація деінкапсулюється і передається одержувачу.

Мережі VPN будуються з допомогою протоколів тунелювання даних через мережу зв'язку загального користування Інтернет. Протоколи тунелювання забезпечують шифрування даних і здійснюють їх наскрізну передачу між користувачами. Для організації мереж VPN використовуються протоколи наступних рівнів: канальний рівень, мережний рівень, транспортний рівень.

На канальному рівні можуть використовуватися протоколи тунелювання даних L2TP і PPTP. Найпоширенішим протоколом VPN є тунельний протокол "точка-точка" PPTP (Point-to-Point Tunneling Protocol), розроблений компаніями 3Com і Microsoft для надання безпечного віддаленого доступу до приватних мереж через Інтернет. Протокол PPTP є розширенням протоколу PPP (Point-to-Point Protocol − протокол «точка-точка») і використовує механізми перевірки автентичності, стиснення і шифрування цього протоколу.

L2TP (Layer2 Tunneling Protocol) − протокол тунелювання другого рівня L2TP не забезпечує шифрування та конфіденційність сам по собі, він спирається на інкапсульований протокол для забезпечення конфіденційності. L2TP використовує засоби шифрування, які надаються методом IPSec. Комбінацію L2TP та IPSec називають L2TP/IPSec. Комбінація L2TP/IPSec забезпечує роботу служб VPN, що виконують інкапсуляцію і шифрування приватних даних.

На транспортному рівні використовується протокол SSL/TLS (Secure Socket Layer/Transport Layer Security), який реалізує шифрування і аутентифікацію між транспортними рівнями приймача і передавача. Для функціонування VPN на основі SSL/TLS немає необхідності в реалізації спеціального програмного забезпечення так як кожен браузер і поштовий клієнт оснащені цими протоколами. У силу того, що SSL/TLS реалізується на транспортному рівні, захищене з'єднання встановлюється «з-кінця-в-кінець».

Реалізація віртуальної приватної мережі практично виглядає так. У локальну обчислювальну мережу офісу фірми встановлюється сервер VPN. Віддалений користувач за допомогою клієнтського програмного забезпечення VPN ініціює процедуру з'єднання з сервером. Відбувається аутентифікація. Далі у разі підтвердження повноважень, між клієнтом і сервером виконується узгодження деталей забезпечення безпеки з’єднання. Після цього організовується VPN-підключення, що забезпечує обмін інформацією між клієнтом і сервером у вигляді, коли кожний пакет проходить через процедури шифрування/дешифрування та аутентифікації даних.

Найімовірніше, основою майбутнього єдиного стандарту буде вже зарекомендований протокол IPSec, який використовується на мережному рівні. Протокол IPSec (Internet Protocol Security) являє собою систему відкритих стандартів, призначених для забезпечення захищених конфіденційних підключень через IP-мережі з використанням криптографічних служб безпеки. Протокол IPSec реалізує шифрування і конфіденційність даних, а також аутентифікацію абонентів. Застосування протоколу IPSec дозволяє реалізувати повнофункціональний доступ, еквівалентний фізичному підключенню до приватної мережі.

Ядро IPSec складають три протоколи: протокол аутентифікації (Authenti-cation Header, AH), протокол шифрування (Encapsulation Security Payload, ESP) і протокол обміну ключами (Internet Key Exchange, IKE).

Для шифрування даних в IPSec може бути застосований будь-який симетричний алгоритм шифрування, що використовує секретні ключі.

На основі аналізу технологій захисту інформації приватних мереж ефективним методом захисту VPN є тунелювання на основі протоколів PPTP, L2TP, IPSec, інкапсульованих в TCP/IP пакетах. Переваги технології VPN у тому, що організація віддаленого доступу робиться не через телефонну лінію, а через Інтернет, що набагато дешевше і краще. Недолік технології VPN у тому, що засоби побудови VPN не є

повноцінними засобами виявлення і блокування атак. Вони можуть запобігти ряду несанкціонованих дій, але далеко не всі можливості, які можуть використовуватися для проникнення в приватну мережу.

Список літератури

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2012.
2. Райан Норман Выбираем протокол VPN [Електронний ресурс]. – Режим доступу: http://www.osp.ru/win2000/2001/07/175027
3. Протоколи і методи реалізації VPN мереж [Електронний ресурс]. – Режим доступу: http://ukrbukva.net/print:page,1,842-Protokoly-i-metody-realizacii-VPN-seteiy.html

УДК 004.056.53

Спосіб організації захищеного каналу передачі даних у системі диспетчеризації технологічними процесами

Буравченко К.О., аспірант,
Минайленко Р.М., канд. техн. наук, доцент
Науковий керівник – Сидоренко В.В., д-р техн. наук, професор
Кіровоградський національний технічний університет, м. Кіровоград

Вступ

Використання бездротового зв'язку для передачі даних від датчиків у системах диспетчеризації технологічними процесами розвивається дуже швидко. Це пов'язано зі стрімким розвитком нових стандартів передачі даних, таких як ZigBee, Xbee, Wi-fi, GPRS та ін. Нові стандарти дають змогу обирати між надійністю, швидкістю та енергоємністю систем передачі даних. Але проблемі захисту інформації у бездротових мережах, які використовуються у технологічних процесах, приділено недостатньо уваги.

Запропоновано метод організації безпечного каналу передачі даних в системі диспетчеризації технологічними процесами з використанням бездротової мережі GSM.

Структура системи збору даних по GSM каналу. Розглянемо систему збору даних від датчиків.

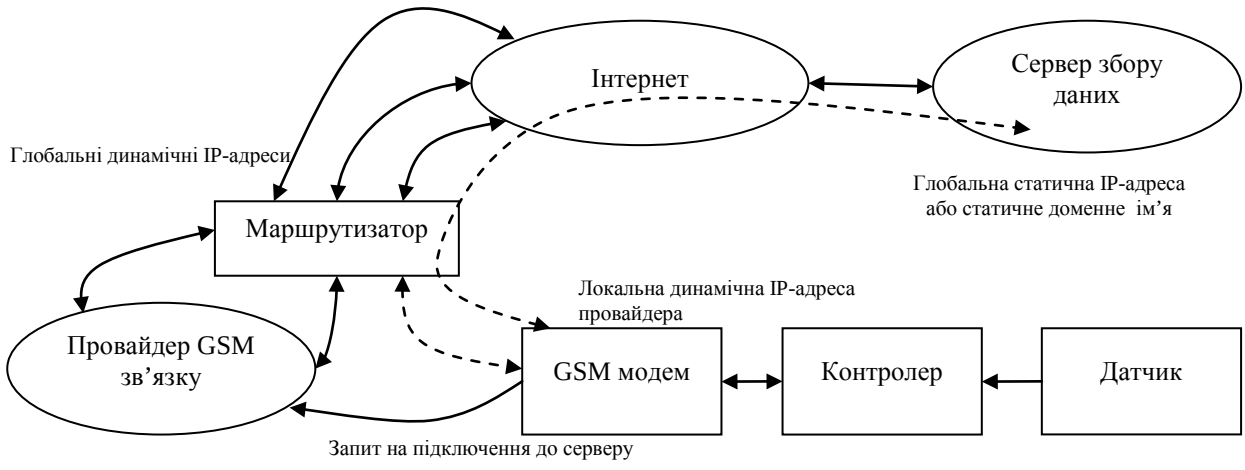

Рисунок 1 – Структурна схема системи збору даних від датчиків на базі GSM-зв'язку

Для віддаленого збору інформації по такій схемі необхідне створення TCP тунелю. Протокол TCP/IP має клієнт-серверну модель і для організації сесії сервер повинен мати статичну IP-адресу або статичне доменне ім'я. Можливі два варіанти організації збору інформації з датчиків: коли вузол збору є TCP-клієнтом або вузол збору є TCP-сервером.

Вузол збору даних – сервер. Коли точка диспетчеризації обрана сервером, необхідно у провайдера мобільного зв'язку отримати статичну глобальну IP-адресу. Враховуючи те, що протокол IPv6 ще не набув широкого розповсюдження і не підтримується більшістю обладнання, а адреси IPv4 поступово закінчуються, то більшість мобільних операторів України видають статичні IP-адреси тільки для великих корпоративних замовників. Тому такий варіант є менш доцільним. Використання динамічної адреси у клієнта та сервера не дозволить створити TCP-сесію, так як такі адреси видають кожен раз випадково і неможливо встановити, яку адресу отримає клієнт чи сервер при наступному підключенні. Фаєрвол оператора мобільного зв'язку маскує трафік, використовуючи локальні таблиці маршрутизації. І тому, якщо навіть ми знаємо динамічну IP-адресу або доменне ім'я GSM-модему, ми не маємо можливості підключитися до вузла збору інформації, тому що відкривається тільки один порт на поточне підключення. Якщо вже створена одна сесія, неможливо відкрити інший порт (фаєрвол блокує), тобто всі дані проходять лише через один порт, відкритий у провайдера.

Вузол збору даних – клієнт. Враховуючи наведене вище, найбільш бажаним варіантом створити TCP-сесію є використання зовнішнього TCP-серверу: наприклад зі статичною адресою або зі статичним доменним ім'ям. Динамічне доменне ім'я можна замовити у провайдера Інтернету або прив'язати його на спеціальних серверах.

Для організації каналу передачі даних у вузлі збору даних часто використовують промислові модеми, які реалізують протокол Modbus. Його мережева модифікація Modbus TCP дозволяє надійно передавати дані без їх втрати. Крім того Modbus є найпоширенішим цифровим протоколом передачі даних у промисловості.

Проблема такої моделі збору даних у тому, що промислові модеми мають статичну програму, яку неможливо віддалено змінити, а канал передачі даних не захищений від атак зловмисників. Дані не шифруються та можуть бути перехоплені як у радіоефірі так і у провайдера мобільного зв'язку.

Іноді для захисту Інтернет трафіку використовують модеми з можливістю побудови Virtual Private Network (VPN), але такий варіант не завжди економічно доцільний.

Алгоритм виходу модему мобільного зв'язку у мережу Інтернет.

1. GSM-модем посилає запит на підключення до TCP-сокету заданого вузла (сайту, серверу, тощо).
2. Якщо сокет недоступний, то TCP-сесія не відкривається, а модем не отримує локальну TCP-адресу.
3. Інакше якщо сокет відкритий, модему видається динамічна IP-адреса у локальній мережі провайдера та відкривається один порт фаєрволу. Цей порт прив'язується до динамічної адреси модему. Далі через цей порт модем має доступ у зовнішню мережу Інтернет. При кожному новому запиті поточний порт закривається і відкривається новий. Крім того шлюз мобільного оператора може мати декілька статичних зовнішніх IP-адрес і багато портів.

Отже серверний сокет, до якого підключається модем, бачить не ту адресу, яку видано GSM-модему динамічно, а лише зовнішній порт та статичну IP-адресу провайдера. Тому навіть знаючи який сокет підключено до сервера, неможливо створити вхідне з'єднання до модему тому, що провайдер не дозволяє зовнішніх вхідних підключень. Це накладає ряд обмежень на перевірку працездатності обладнання та мережі збору інформації в цілому. Не дає можливості навіть перевірити доступність хоста за допомогою ICMP запитів.

Організація захищеного каналу за допомогою Reverse SSH

Запропоновано спосіб, який дозволяє використовуючи одноплатний комп'ютер, наприклад Raspberry Pi з встановленою операційною системою Linux, організувати захищений канал збору даних від віддалених пристроїв. Для реалізації віддаленого керування та захищеного каналу обрано широко вживаний протокол Secure Shell (ssh).

1. На центральному сервері диспетчеризації (Точка А) відкривають ssh-сервер.
2. Одноплатний комп'ютер (Точка Б) виступає в ролі ssh-клієнта і ініціює з'єднання по протоколу ssh до А, але крім того також має можливість прийому ssh-клієнтів; створюючи реверсивний ssh канал.
3. Після ініціалізації з'єднання на А за допомогою вбудованих можливостей ssh комутуються порти 22 (ssh) точки Б та деякий порт N точки А, вказаний у налаштуваннях.
4. На комп'ютері А запускають віддалений термінал до Б, використовуючи створений порт N. Тобто Б і А змінюються місцями, а використовується та ж сама TCP-сесія.

Даний спосіб дозволяє отримати доступ до ресурсів клієнта після того, як він підключається до сервера. Далі клієнт і сервер змінюються місцями, тому він і називається реверсивний ssh.

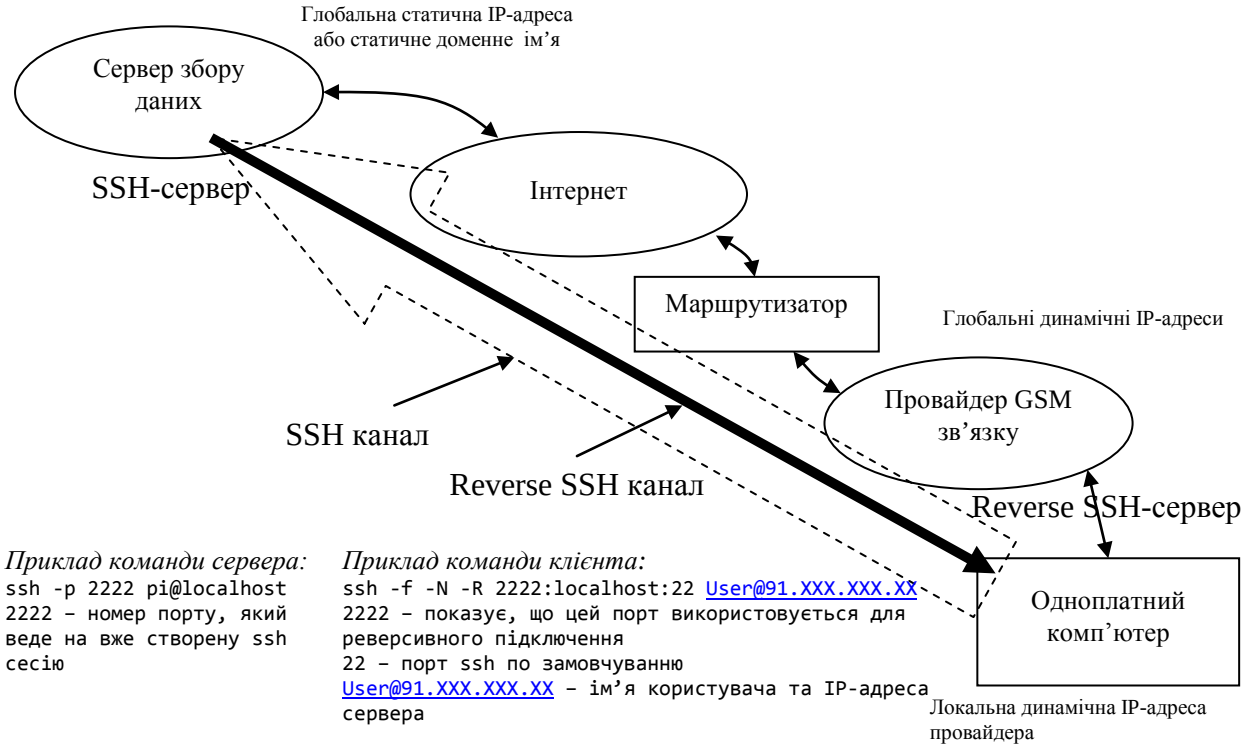

Рисунок 2 – Схематичне зображення способу організації захищеного каналу передачі даних на базі GSM-зв'язку за допомогою SSH протоколу

Переваги запропонованого способу:

- шифрований канал.
- використання віддаленого терміналу для переконфігурації пристрою, збору налаштувань і таке інше.
- при достатньо високій швидкості використання Інтернет з'єднання можливе використання Virtual Network Computing.
- кросплатформеність. Протокол ssh реалізований в багатьох операційних системах.
- непотрібно використання проміжних серверів та виділення у провайдера зв'язку статичної IP-адреси.

До недоліків можна віднести недоліки, які виникають при використанні бездротової мережі. Тобто при використанні такої мережі будуть обриви зв'язку і т.д. Для подолання цього недоліку можна архівувати дані на стороні клієнта і потім пакетом передавати їх на сервер.

Висновки. Показано проблему, яка виникає при організації збору даних від датчиків по GSM-каналу, а саме проблема створення захищеної TCP-сесії. Запропоновано спосіб організації захищеного каналу передачі даних у таких системах на основі протоколу SSH.

Список літератури

1. OpenSSH [Електронний ресурс]. – Режим доступу: http://www.openssh.com/
2. Secure Shell, SSH [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/SSH
3. Проблемы передачи данных в сетях мобильной связи [Електронний ресурс]. – Режим доступу: http://www.ccc.ru/magazine/depot/02_05/read.html?0302.htm
4. Козлов А. Промышленные стандарты беспроводной передачи данных // Chip News Украина. – 2008. – №7. – С. 18-21
5. Романов В.О., Галелюка І.Б., Груша В.М., Чернега П.П. Розподілена система збору і обробки інформації на базі інтелектуальних портативних приладів. // Комп'ютерні засоби, мережі та системи. – 2009, №8. – С. 64-72

УДК 681.3.07

"SaaS" як надійний метод захисту програмного забезпечення

Глінський Б.В., студент 5 курсу
Науковий керівник – Павлов В.Г., канд. техн. наук, доцент
Національний авіаційний університет, м. Київ

У наш час розвиток інформаційних технологій призвів до створення величезної кількості програмного забезпечення, яке є результатом творчої діяльності людей, та на яке поширюються права інтелектуальної власності. Тому ці програми повинні мати надійний захист від неліцензійного використання, яке, на жаль, дуже поширено у світі, зокрема, в Україні.

Більшість захисних механізмів реалізовано у вигляді вбудованого програмного коду. Це обмежує можливість неліцензійного використання ПЗ, але не обмежує доступу до самих програм. Тому зловмисник може за допомогою спеціальних програм-відладчиків усіляко досліджувати дане ПЗ, а саме: дивитися код програми у статичному стані, аналізувати залежності даних, вислідковувати їх переміщення, досліджувати виконання програмних інструкцій у покроковому режимі (трасування) тощо. Тому, врешті – решт цей захисний механізм досліджується з метою його знищення або відключення. Технологія "SaaS" (software as a service) передбачає надання доступу до програмного забезпечення за допомогою WEB-інтерфейсу, що виключає безпосередній контакт користувача з програмним кодом.

Моделі хмарного розміщення.

Приватна хмара (private cloud) – це модель «хмарного» розміщення, в якій постачальник послуг і споживачі належать одній організації.

Публічна хмара (public cloud) – модель «хмарного» розміщення, в якій постачальник і споживачі послуг належать різним організаціям.

Громадська хмара (community cloud) – модель «хмарного» розміщення, відповідно до якого ресурси використовуються конкретною спільнотою споживачів з організацій, що мають спільні завдання.

Гібридна хмара (hybrid cloud) – модель «хмарного» розміщення, в якій об'єднані дві і більше cloud-інфрастуктури, що належать різним організаціям або типам моделей (приватним, громадським чи публічним). Вони залишаються унікальними об'єктами, але пов'язані між собою стандартизованими чи приватними технологіями передачі даних і додатків.

Розподілена хмара (distributed cloud) – модель, яка забезпечується набором машин, які працюють з різних місць і одночасно підключені до єдиної мережі.

Міжхмарна модель (intercloud) – зв'язана глобальна «хмара хмар» і розширення Інтернету (мережі мереж), на яких вона базується.

Мультихмара (multicloud) – модель, яка використовує багатократні послуги по хмарним обчисленням в єдиній різнородній архітектурі.

Класифікація «хмар» відповідно до рівнів.

Так як концепція «хмари» заснована на рівнях, кожен з яких надає певну послугу і функціональність, то необхідно провести їх класифікацію: програмне забезпечення як послуга, обладнання як послуга, комп'ютер як послуга, робоче оточення як послуга, дані як послуга, комунікація як послуга, моніторинг як послуга, інфраструктура як послуга, платформа як послуга, безпека як послуга, все як послуга.

Основні атаки.

Традиційні атаки на ПЗ – пов'язані з уразливістю мережевих протоколів, операційних систем, модульних компонент та інших.

Функціональні атаки на елементи «хмари» - пов'язані з багатокомпонентністю «хмари», загальним принципом безпеки, який полягає в тому, що загальний захист системи дорівнює захисту найслабшої ланки.

Атаки на клієнта – такі атаки як Cross Site Scripting, перехоплення веб-сесій, крадіжка паролів та інші.

Загрози віртуалізації – оскільки платформою для «хмар» є віртуальні середовища, то атаки на систему віртуалізації також загрожують і всьому cloud-середовищу в цілому.

Втрата даних – можлива через природні катаклізми, воєнну ситуацію, збої в енергопостачанні, виході обладнання з ладу тощо.

Викрадення трафіку - отримання зловмисником доступу до облікових даних надає йому можливість маніпулювати внутрішнім середовищем cloud-системи.

Зловживання можливостями «хмар» - наприклад, хтось може скористатися обчислювальними потужностями для того, щоб зламати пароль до архіву.

Основні напрями захисту з використанням методу "SaaS".

Фізичний захист: кліматконтроль обладнання, протипожежні засоби, забезпечення безперебійного постачання, біометричні та інші способі контролю тощо.

Безпека мережі і логічний поділ: використання віртуальних версій фаєрволів і IDS, ізоляція критичних секцій.

Адміністрування: наявність різних рівнів мережевих адміністраторів, обмеження до доступу «хмарного середовища», відключення непотрібних сервісів, API тощо.

Всебічний моніторинг та реєстрація: моніторинг та контроль доступу до мереж, систем, програм та даних.

Безпека додатків і даних: використання додатками тільки виділених баз даних, доступ до баз даних через програми повинен бути обмежений.

Аутентифікація і авторизація: обов'язковість при віддаленому і будь-якому іншому привілейованому доступі. Чітке розділення ролей користувачів, адміністраторів тощо.

Управління вразливостями: захист програмних клієнтів, сервісів тощо від відомих вразливостей.

Зберігання даних: сортування різних типів даних, фізичне і логічне їх розмежування.

Шифрування: шифрування даних в момент передачі і зберігання, наприклад зберігання на сервері не відкритого паролю, а його зашифрований вигляд.

Отже, зважаючи на вищезазначене, можна сказати, що на даний час метод "SaaS" є найбільш дієвим та перспективним методом захисту ліцензійного програмного забезпечення. Значно менша вартість користування ліцензійним ПЗ з одночасною цілодобовою сервісною підтримкою роблять безглуздими проведення атак на програмний код, оскільки стають економічно недоцільними. Для тих же зловмисників, які все ж наважуються викрасти програмний код, використання технологій "SaaS" створює неабиякі труднощі.

УДК 004.056.5

Розробка підходу оцінки кіберризиків в корпоративних комп'ютерних мережах

Завгородній К.Р., аспірант
Науковий керівник – Захарова М.В., канд. техн. наук, доцент
Черкаський державний технологічний університет, м. Черкаси

Оцінка ризику – це процес вирішення задачі пошуку оптимальних значень рівнів ризику компрометації інформаційних ресурсів. Одним із способів розв'язку задач такого класу є залучення експертів з інформаційної безпеки та на основі їх рекомендацій визначення рівня ризику. В інших випадках визначення цього параметру проводиться на основі аналізу статистичних даних про інциденти порушення інформаційної безпеки організації. В такому випадку оцінка ризику визначається на основі кількості атак за виділений проміжок часу або на основі співвідношення успішних атак до неуспішних.

Кіберризики (електронні ризики) – це множина ризиків, що включають в себе можливість крадіжки, несанкціонованого доступу, заміни чи знищення інформації організацій, що використовують в процесі ведення бізнесу корпоративні мережі. Сукупність інформації різного роду в таких мережах називається інформаційними ресурсами.

Помилкова оцінка ризику може призвести до негативних наслідків, а саме: матеріальні збитки організації, погіршення іміджу, відповідальність перед законом, тощо. Тому необхідність в точних розрахунках постає гострою проблемою в процесі прийняття рішень в управлінні інформаційною безпекою. На результати процесу оцінки ризику мають великий вплив суб'єктивні фактори експерта з інформаційної безпеки, зокрема: рівень кваліфікації експерта, його особисті переконання та професійні якості. Статистичні дані взагалі можуть бути відсутні, так як не кожна організація веде таку статистику. Підвищення точності результату процесу оцінки ризику є актуальною проблемою, тому метою даної роботи є розробка підходу оцінки кіберризиків для корпоративних мереж, що додатково враховує фактори зовнішнього середовища та мінімізує вплив суб'єктивного фактору.

Рівень кіберризику R для інформаційного ресурсу I корпоративної мережі (ІРКМ) визначається у співвідношенні:

$$R = Z * U, \quad (1)$$

де U - потенціальні збитки, Z – ймовірність реалізації загрози. Ймовірність реалізації загрози випливає з наявних в системі інформаційної безпеки вразливостей.

Перед початком роботи над процесом оцінки ризику проводиться аналіз інформаційних ресурсів корпоративних мереж. Цей процес включає в себе опис всіх наявних інформаційних ресурсів в системі з зазначенням їхньої цінності та значимості. Маючи перелік ІРКМ, що потребують захисту, потрібно виконати пошук вразливостей, характерних для компонентів даної мережі. Вразливість – це будь-яка властивість чи характеристика мережі, використання якої порушником, може призвести до реалізації загрози. Задача пошуку вразливостей є складною для розв'язання. Для її вирішення розроблено велику кількість програмних продуктів, таких як: Nessus, xSpider, Nikto2, Network Hotfix Scanner, IronWISP та ін. Наведені програмні продукти (ПП) та подібні відносяться до класу мережевих сканерів. Використання таких ПП вимагає високих професійних навичок користувача. Результатом роботи сканерів є множина вразливостей, наявних в системі інформаційної безпеки об'єкта сканування.

Зловмисник, маючи відомості про вразливості, наявні в системі безпеки, та, при наявності достатніх умінь і технічних засобів, може здійснити несанкціонований доступ до

системи з високою ймовірністю. В такому випадку ймовірність реалізації загрози буде наближатися до 1. Потрібно враховувати складність реалізації загрози, яка характеризується вимогами до рівня кваліфікації злочинця. Складність реалізації загрози L може бути: високою (від 0.8 до 1), середньою (від 0.5 до 0.8), низькою (від 0.2 до 0.5) та незначною (від 0 до 0.2) [1]. Для реалізації загрози високого рівня складності зловмиснику потрібно мати фундаментальні знання системної організації ресурсів, протоколів зв'язку, для середнього – знання операційних систем, низького - знання мов програмування, низького – елементарні знання в області обчислювальної техніки. Інформація про рівні складності реалізації загроз має вільний доступ, наприклад бюлетені безпеки Microsoft [2]. Враховуючи це, рівень загрози здійснення атаки через наявну вразливість V, буде визначатися таким чином:

$$Z_V = 1 - L_V \tag{2}$$

Те, що в системі захисту інформаційних ресурсів присутні вразливості , ще не означає, що ними хтось скористується. Ризик їх використання збільшується тоді, коли підприємство має досить тверду позицію на ринку та веде вдало конкурентну боротьбу. Одним з факторів, яким можна описати конкурентоспроможність компанії, є коефіцієнт конкурентоспроможності K_k[2]. Цей параметр має прямий вплив на Z, тому

$$Z_V = (1 - L_V) * K_k \tag{3}$$

Суттєвий вплив на рівень ризику має значення потенціалу зловмисника P . Цей фактор визначається на основі статистичних даних про здійснені атаки на досліджуваний інформаційний ресурс. Такі статистичні відомості, з тих чи інших причин, не завжди доступні. При наявності достатніх навичок на основі аналізу даних журналів операційної системи можна відтворити відомості про ідентифіковані атаки на систему та їхню успішність. За умови, що статистичні дані наявні, потенціал зловмисника P_V визначається за відношенням кількості успішних атак до їх загальної кількості. В іншому випадку цей параметр не використовується. Отже:

$$P_V = \frac{p_s}{p_m}, \tag{4}$$

де p_s - кількість успішних атак, p_m - загальна кількість атак.

Тоді, визначення рівня загрози атаки через конкретну вразливість є таким:

$$Z = (1 - L_V) * K_k * P_V. \tag{5}$$

В організації ІРКМ, як правило, мають більше одної вразливості, через які можливо здійснити атаку на компрометацію цього ресурсу. Тому доцільно визначити загальний рівень ймовірності реалізації загрози, де в результаті ми отримаємо рівень загрози, що хоча б одна атака буде успішною. В такому випадку формула має вигляд:

$$Z_I = 1 - \prod_{V=1}^{n}\big((1 - L_v) * K_k * P_v\big). \tag{6}$$

Таким чином, запропонований підхід дозволяє оцінювати кіберризики шляхом урахування впливу зовнішніх факторів та максимального зменшення суб'єктивного фактору, що дозволить підвищувати ефективність прийняття рішень в управлінні безпекою інформаційної системи, що підвищує безпеку ведення бізнесу та позитивно позначається на економічному кліматі організації.

Список літератури

1. Корченко, А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. / А. Г. Корченко – К.: «МК-Пресс», 2006. – 320 с.

2. Бюлетень безпеки Microsoft./Microsoft. – Доступ до ресурсу: http://technet.microsoft.com/ru-ru/security/bulletin

3. Пастухова Т. Ю. Метод розрахунку конкурентоспроможності підприємства, заснований на теорії ефективної конкуренції: матеріали VII міжнародної науково – практичної інтернет конференції ["АЛЬЯНС НАУК: ВЧЕНИЙ – ВЧЕНОМУ"] Т.1, (15 – 16 березня, 2012 р.)/ Інститут проблем ринку та економіко-екологічних досліджень НАН України.-Дніпропетровськ, 2012. - 36-40с.

УДК 004.514.62

Засоби реалізації критеріїв спостережності в комп’ютерних системах

Зозуля Я.В., студент 5 курсу
Науковий керівник – Томашевський В.В., старший викладач
Житомирський військовий інститут Державного університету телекомунікацій, м. Житомир

Автономно працюючий комп’ютер можна ефективно захистити від зовнішніх атак різними засобами. Комп’ютер, що працює в мережі, по визначенню не може бути повністю відключений від світу, він повинен «спілкуватися» з іншими комп’ютерами, можливо, навіть віддаленими від нього на великі відстані. Саме тому забезпечення безпеки в мережі являється завданням значно більш складнішим. Логічний вхід користувача в комп’ютер являється штатною ситуацією, якщо робота відбувається в мережі. Забезпечення безпеки в цій ситуації зводиться до того, щоб зробити це проникнення контрольованим – кожному користувачу мережі повинні бути чітко присвоєні його права для доступу до інформації, зовнішнім пристроям і виконанню системних дій на кожному з комп’ютерів мережі.

Забезпечення захисту реалізується за допомогою служб захисту – сукупності механізмів, процедур та інших управляючих дій, що реалізовані для зменшення ризику, зв’язаного з загрозою. Коректність роботи служби захисту визначається рядом процедур, таких як аутентифікація, ідентифікація, авторизація, аудит та іншими.

Сучасні загрози безпеці інформації можна подолати, вразливості можна усунути, і в цілому завдання забезпечення захисту ресурсів в складних умовах виконується, якщо тільки грамотно експлуатувати та підтримувати систему безпеки. Це полягає у проведенні цілого комплексу неперервних і періодичних робіт, таких як технічна підтримка засобів захисту, моніторинг та аналіз подій безпеки, що відбуваються в системі, періодичний контроль захищеності ресурсів, подолання нештатних ситуацій та ліквідація наслідків.

В нинішній час актуальними є проблеми безпеки та адміністрування комп’ютерних систем, такі як контроль діяльності, реагування на події, створення звітності, мінімізація простоїв роботи систем. На допомогу приходять програми віддаленого адміністрування, що дозволяють отримати віддалений доступ до комп’ютера в локальній мережі або через Інтернет.

У проекті вирішено задачу побудови системи взаємодії клієнта з сервером для віддаленого управління та моніторингу робочими станціями, визначено алгоритм мережевої взаємодії, розроблено програмне забезпечення серверної та клієнтської частини програмного комплексу. Функції віддаленого доступу забезпечують отримання інформації про систему, інформації диспетчера завдань, монітору ресурсів, файлового менеджера. Забезпечена можливість перегляду та управління робочим столом.

Під час розробки проекту спиралися на функціонал таких потужних програм як Radmin, Splashtop, Remote Desktop, TeamViewer. Для побудови програмного продукту використовували систему побудови клієнтських застосувань Windows Presentation Foundation (WPF). Використовували технологію Windows Management Instrumentation (WMI) для централізованого управління та слідкування за роботою різноманітних частин комп'ютерної інфраструктури. Для обміну даними використовували програмний інтерфейс сокетів Берклі та текстовий формат обміну даних JavaScript Object Notation (JSON), що використовувався для маршалізації (серіалізації) об'єктів.

Розроблений програмний комплекс дозволяє працювати на віддаленому комп'ютері в

режимі реального часу, що дозволяє зменшувати затрати на обслуговування масштабних інформаційно-телекомунікаційних систем, а також збільшує рівень захищеності системи вцілому, шляхом впливу на такі властивості інформації як доступність та спостережність.

Список літератури

1. Приемы объектно-ориентированного проектирования. Паттерны проектирования / Э. Гамма, Р. Хелм, Р. Джонсон, Дж. Влиссидес. – СПб.: Питер, 2001. – 368 с.
2. Паттерны проектирования / Э. Фримен, Э. Фримен, К. Сьерра, Б. Бейтс. – СПб.: Питер, 2011. – 656 с.
3. Рихтер Дж. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.0 на языке C#. 3-е изд. / Дж. Рихтер. – СПб.: Питер, 2012. – 928 с.
4. Троелсен Э. Язык программирования C# 2010 и платформа .NET 4.0, 5-е изд. / Э. Троелсен.–Пер. с англ. – М.: ООО «И.Д. Вильямс», 2011. – 1392 с.
5. Натан А. WPF 4. Подробное руководство / А. Натан. – Пер. с англ. – СПб.: Символ-Плюч, 2011. – 880 с.

УДК 681.3

Модель системи інформаційної безпеки

Кавун С.В., канд. техн. наук, доцент
Харківський інститут банківської справи Університету банківської справи Національного банку України

Під захищеністю ІС підприємства будемо розуміти ступінь адекватності реалізованих у ній механізмів захисту інформації, існуючої в даному середовищі функціонування ризикам, пов'язаним із здійсненням загроз безпеки інформації. Під погрозами безпеки інформації підприємства традиційно розуміється можливість порушення таких властивостей інформації, як конфіденційність, цілісність та доступність.

Основою формального опису систем захисту традиційно вважається модель системи захисту з повним перекриттям, у якій розглядається взаємодія "області погроз", "захищаємі області" – ресурси ІС та "системи захисту" – механізми безпеки ІС [3].

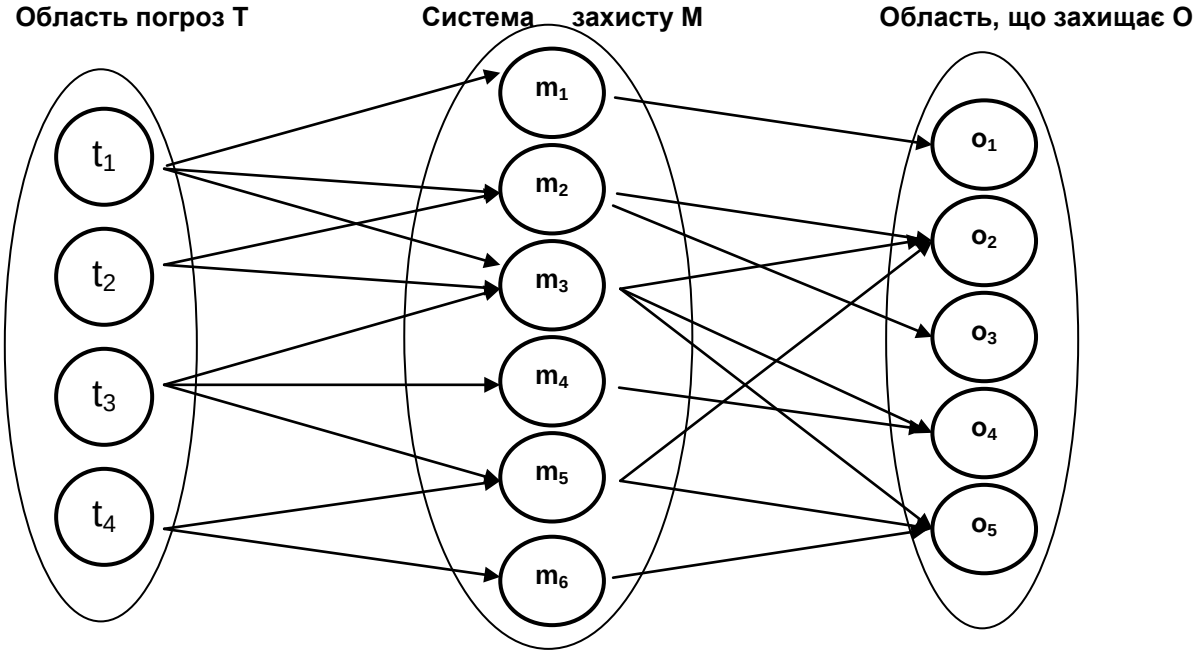

Рисунок 1 – Модель графа Q_2 системи інформаційної безпеки підприємства з повним перекриттям

Таким чином, маємо три множини:

T = {t_i} - множина погроз безпеки,

O = {o_j} - множина об'єктів (ресурсів) захищеної системи,

M = {m_k} - множина механізмів безпеки.

Елементи цих множин перебувають між собою в певних відносинах, які властиво й описують систему інформаційної безпеки підприємства.

Для опису системи інформаційної безпеки підприємства звичайно використовується модель графа, яка представлена на рис. 1.

Множина відносин типу погроза-об'єкт утворює дводольний граф **Q_1 {<T, O>}**. Ціль захисту полягає в тому, щоб перекрити всі можливі ребра в графі. Це досягається введенням третьої множини **M**. У результаті виходить тридольний граф **Q_2 {<T, M, O>}**.

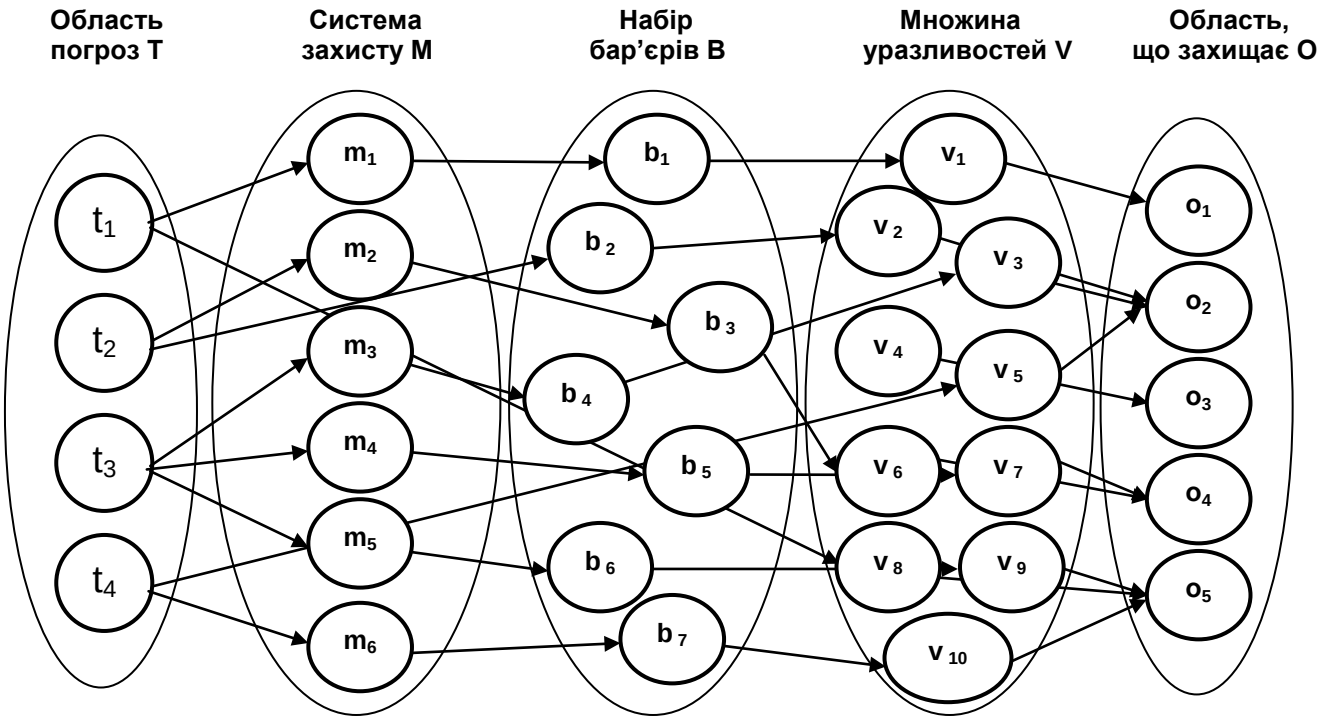

Рисунок 2 – Модель графа Q_3 системи інформаційної безпеки підприємства, що містить уразливості

Подальший розвиток моделі припускає введення ще двох множин:

V - набір уразливих місць, обумовлений підмножиною декартового добутку **T×O**: $\mathbf{v}_r$ = <$\mathbf{t}_i$, $\mathbf{o}_j$>. Таким чином, під уразливістю системи інформаційної безпеки підприємства будемо розуміти можливість здійснення погрози $\mathbf{t}_i$ відносно об'єкта $\mathbf{o}_j$ (на практиці під уразливістю системи інформаційної безпеки підприємства звичайно розуміють не саму можливість здійснення погрози безпеки, а ті властивості системи, які сприяють успішному здійсненню погрози, або можуть бути використані зловмисником для здійснення погрози);

B - набір бар'єрів, обумовлений декартовим добутком **V×M**: $\mathbf{b}_l$ = <$\mathbf{t}_i$, $\mathbf{o}_j$, $\mathbf{m}_k$>, що представляють собою шляхи здійснення погроз безпеки, які перекриті засобами захисту.

У результаті одержуємо систему, що складається з п'яти множин: Q_3 {<**T**, **O**, **M**, **V**, **B**>}, й яка описує систему інформаційної безпеки підприємства з урахуванням наявності в ній уразливостей, яка наведена на рис. 2.

Список літератури

1. Майника Э. Алгоритмы оптимизации на сетях и графах: Пер. с англ. - М. Мир, 1981. - 323 с.
2. The ISO 17799 Service & Software Directory.
3. http://www.iso17799software.com.

УДК 004.056.55

Переваги та недоліки використання IPSec у VPN

Кікоть В.М., студент 5 курсу
Науковий керівник – Резніченко В.А., викладач
Кіровоградський національний технічний університет, м. Кіровоград

Багато організацій по всьому світу для зв'язку своїх окремих офісів використовують всілякі методи їх фізичного з'єднання. Це можуть бути як виділені цифрові лінії, так і VPN - Virtual Private Networks, які значно дешевші їх фізичних аналогів. Використовуючи, загалом, ті ж підходи, що і виділені лінії, VPN можуть об'єднувати кілька локальних мереж в одну і шифрувати трафік для приховування переданої інформації. У разі використання шифрування в технології VPN, як правило, застосовуються відкриті стандарти. При цьому трафік передається поверх IP і використовує в якості транспортного рівня датаграми.

Технічно організація VPN може бути виконана як програмними засобами, так і апаратними. Ці рішення функціонують як маршрутизатори на кінцях VPN-з'єднань. При передачі клієнтом пакету, він пересилає його на цей спеціалізований маршрутизатор, який додає до пакету заголовок перевірки автентичності (Authentication Header, (AH)). Після кодування цих даних і додавання до них інструкцій з декодування і обробки, вони передаються на інший кінцевий спеціалізований маршрутизатор, що приймає ці пакети. Після прийому пакета, кінцевий маршрутизатор розкодує його, відкидаючи заголовок, і передає пакет кінцевому користувачеві за місцем призначення.

У глобальному сенсі IPSec - це "каркас", який є частиною продуктів, що вимагають наступної функціональності: організація захищеного з'єднання між точкою А і точкою В. Використовуючи потужне шифрування і криптування на основі публічних ключів, IPSec може забезпечити захист з'єднань від несанкціонованого доступу.

IPSec являє собою набір алгоритмів і протоколів з досить гнучкою внутрішньою структурою, що дозволяє виробникам різних пристроїв, що підтримують IPSec, самостійно вибирати оптимальні з їхньої точки зору ключі, алгоритми та методи аутентифікації.

Найбільш типове застосування IPSec для досягнення конфіденційності та цілісності даних при їх транспортуванні по незахищеним каналам. Спочатку IPSec призначався для захисту даних в публічних мережах, проте його різні практичні реалізації нерідко використовуються для збільшення безпеки приватних мереж.

Хоча IPSec найбільш популярне і, мабуть, найкраще рішення для створення віртуальних приватних мереж, є і деякі обмеження. У разі його застосування в транспортному режимі не виключається можливість атак ззовні, що викликано деякими обмеженнями протоколу ISAKMP.

Злом сесії IPSec цілком вірогідний, якщо не використовується заголовок аутентифікації AH. За такого типу атаки дані зловмисника можуть бути вставлені в інформацію, що передається, щоб одержувач в підсумку втратив деякі або всі файли на жорсткому диску.

Оскільки трафік IPSec маршрутизуємий, різні практичні реалізації IPSec можуть піддатися більш "витонченій" атаці - підміні початкового маршруту. Даний вид атаки можливий лише при використанні IPSec в транспортному режимі, якщо ж він застосовується для побудови тунелю, вся роутингова інформація в цьому випадку шифрується і подібний вид атаки успіху не матиме.

Фахівці компанії AT&T Research відзначають, що багато потенційно слабких місць IPSec є наслідком певних недоліків алгоритмів шифрування, використаних в конкретній реалізації IPSec. Отже, зі збільшенням надійності цих алгоритмів IPSec може стати набагато більш захищеним.

В даний час IPSec - це частина IPv6, але не IPv4. Хоча, звичайно ж, є й реалізації IPSec для протоколу IP четвертої версії. У реалізації для IPv6 деякі слабкі місця IPSec, які все ж присутні у версії для IPv4, усунені. Так, наприклад, поля фрагментації в заголовку пакета IPv4 потенційно можуть бути змінені, тому при функціонуванні IPSec в транспортному режимі зловмисник може перехопити пакет і змінити поле фрагментації, а потім вставити необхідні дані в переданий потік. В IPv6 ж проміжні маршрутизатори не допускають зміни полів фрагментації.

Протокол IPsec домінує в більшості реалізацій віртуальних приватних мереж. В даний час на ринку представлені як програмні реалізації (наприклад, протокол реалізований в операційній системі Windows2000 компанії Microsoft), так і програмно-апаратні реалізації IPsec - це рішення Cisco, Nokia. Незважаючи на велику кількість різних рішень, всі вони досить добре сумісні один з одним.

Технологія IPSec отримує вкрай неоднозначні оцінки фахівців в галузі безпеки. З одного боку, наголошується, що протокол IPSec є кращим серед всіх інших протоколів захисту переданих по мережі даних, розроблених раніше (включаючи розроблений Microsoft PPTP). З іншого боку, присутня надмірна складність і надлишковість протоколу - це в принципі не критично, але деякі спеціалісти зазначають, що є серйозні проблеми безпеки практично у всіх головних компонентах IPSec.

Список літератури

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2012.
2. Олифер В. Г.,Олифер Н. П. Глава 24. Сетевая безопасность // Компьютерные сети. Принципы, технологии, протоколы. — 4-е. — СПб: Питер, 2010. — С. 887-902. — 944 с.
3. Andrew Mason. IPSec Overview. — Cisco Press, 2002.
4. Bollapragada V., Khalid M., Wainner S. - IPSec VPN design (2005)

УДК 004.056.57

Захист від шкідливих програм за допомогою системних засобів

Левошко О.Л., старший викладач
Кіровоградський національний технічний університет, м. Кіровоград

Програми, призначені для маскування мережевих з'єднань, процесів і дискових файлів, а також інших програм називають руткітами. Існують два типи руткітів: перші створюють нові файли або модифікують вже існуючі, другі обмежуються модифікацією оперативної пам'яті.

Маскування системних програм базується на модифікації структур даних або системного коду. Таблиці глобальних та локальних дескрипторів (GDT/LDT) зберігають базові адреси, межі та атрибути селекторів. Для захисту від руткіта створюється новий селектор з базою, відмінною від нуля, з подальшим його завантаженням до одного з сегментних регістрів. Побічним ефектом даного прийому стає поява нових селекторів в таблиці дескрипторів.

Частина руткітів модифікує таблицю дескрипторів переривань (IDT), що дозволяє їм перехоплювати будь-які переривання та виключення, в тому числі і системні виклики. Модифікація IDT дозволяє руткіту перехоплювати такі виключення, як, наприклад, загальне виключення захисту (General Protection Fault), звернення до сторінок та апаратні

переривання. Для контролю вмісту таблиці переривань використовується процесорна команда SIDT, оскільки перехопити її виконання руткіт не в змозі. Руткіт може модифікувати таблиці дескрипторів переривань, замінюючи вектор 80h на свій власний код. Переривання INT 80h передає управління на функцію system_call. Руткіт або читає вектор 80h через SIDT, або знаходить system_call евристичним шляхом, оскільки вона містить досить характерний код. Вставивши на початок (або середину) цієї функції команду переходу на своє тіло, руткіт буде отримувати управління при будь-якому системному виклику. Отже, потрібно вилучити код функції system_call з пам'яті, порівнявши його з оригіналом, який можна взяти з дистрибутивного диска. Після виконання системного виклику управління отримує функція ret_from_sys_call, що йде слідом за system_call. Її перехоплюють багато руткітів. Команда SYSENTER передає управління з третього кільця прикладного рівня на ядерний рівень, використовуючи спеціальні MSR-регістри: IA32_SYSENTER_CS містить селектор сегмента, IA32_SYSENTER_EIP – адресу переходу, IA32_SYSENTER_ESP – нове значення регістра ESP при переході на ядерний рівень. Відобразити вміст регістрів MSR можна командою RDMSR, яку руткіт також не може перехопити.

Отже, для захисту від руткіта потрібно контролювати код системних функцій system_call та ret_from_sys_call та використовувати швидкий механізм системних викликів, реалізований командами SYSENTER/SYSEXIT, SIDT, RDMSR.

Список літератури

1. Дмитрий Олексюк, Esage Lab Обнаружение руткитов режима ядра с помощью отладчика / В.К. Дмитрий Олексюк, Esage Lab

2. Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 2B: Instruction Set Reference, N-Z [Електронний ресурс]. – Режим доступу: http://www.intel.com/content/www/us/en/architecture-and-technology/64-ia-32-architectures-software-developer-vol-2b-manual.html

УДК 004.056.5

Види зламів веб-сайтів та методи запобігання їм

Ломакін В.В., студент 3 курсу
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

На сьогоднішній день існує безліч технологій та мов програмування, за допомогою яких програміст має змогу створити веб-сайт або веб-додаток. З розвитком технологій з'являються нові способи для зламу сайтів. В даній роботі розглядаються веб-сайти, написані на мові програмування PHP з використанням бази даних MySQL. Чому саме PHP? Тому що переважна більшість веб-сторінок створена за допомогою PHP. Це пояснюється тим, що технологія досить проста та зручна в використанні. Простота та зручність є як плюсом для створення веб-сторінок, так і великим мінусом. І іноді це занадто великий мінус, оскільки зворотною стороною простоти є слабка система захисту.

В сучасному світі неможливо обійтись без PHP і більшість веб-сайтів написано завдяки цій технології. Розглянемо детальніше способи захисту від зламу таких сайтів. PHP – виконується на сервері, а в браузер користувача повертається html-код. Здавалося б, що це досить надійно, проте, можливі атаки на веб-сервер, що повернуть вам вже неправильний html-код сторінки. Один із поширених видів атаки проводиться через форми html. Це пояснюється тим, що форма обробляється сервером, саме тому хакер може вводити неправильні, хибні дані в форми. Часто в форму пишеться sql-ін'єкція – це особливий запит, який деструктивно діє на базу даних. Цей запит змінює sql-запит та дозволяє отримати інші

закриті дані. Зокрема такий спосіб використовується для зламу реєстрації, де є спеціалізована форма вводу, наприклад, логіна і паролю. Замість логіну вводиться запит, цей запит оброблюється сервером і може повернути всі записи з бази даних, такі як логін і пароль адміністратора. Після цього хакер розширює свої права до прав адміністратора. Такого не можна допустити, слід заздалегідь закрити можливість для подібних атак. Саме тому для захисту сценарію потрібно перевіряти кожний параметр, який прийшов від користувача, та забороняти всі небезпечні символи, як одинарні лапки, подвійні лапки та знаки відкриття та закриття тегів. Неможливо заборонити кожний html-тег, ви обов'язково щось забудете. Та навіть, якщо перечислити всі теги, то з новими версіями html з'являться нові теги. Тому слід використовувати регулярні вирази. За допомогою них можна перевірити кожний параметр, який приходить з форми.

Розглянемо детальніше основні способи зламу веб-сайтів та методи захисту від них.

Завантаження файлів

Сайт може дозволяти відвідувачам завантажувати свої файли з подальшим відображенням на своїх сторінках. Це можуть бути, наприклад, зображення у форматі JPEG. Важливо обмежити типи файлів, що завантажуються, щоб замість картинки не був би завантажений виконуваний файл. При завантаженні файлу PHP в змінній $_FILES ['userfile'] ['type'] повертає mime-тип файлу, для JPEG-зображення це буде image/jpeg. Може здатися, що перевірка цього типу достатня для впевненості в тому, що завантажено саме зображення. Також зустрічається ідея намагатися читати файл зображення функціями getimagesize або imagecreatefromjpeg. Однак тип файлу тут визначається на основі змісту, так що правильне JPEG-зображення, збережене з розширенням .php, буде визначено як image/jpeg. А називатися буде xxxxx.php. Веб-сервер же, який приймає рішення про обробку (handler) для того чи іншого файлу, дивиться саме на розширення. Зловмисник бере коректну картинку, приписує до неї в кінець (або в EXIF-дані) php-скрипт, і сервер його виконує, веб-сайт зламано. Таким чином, контролювати для забезпечення безпеки слід саме розширення файлу, а перевірки через визначення mime-type і через спробу відкрити файл функцією getimagesize мають сенс тільки для контролю того, що замість картинки не буде завантажене сміття, нешкідливе, але картинкою яке не є.

Register Globals

У PHP є функціональність "Register Globals" - автоматичне закладання змінних при надходженні їх в запиті (GET, POST, COOKIE). Тобто, наприклад, скрипт <?php echo $a;?>, будучи викликаний, як script.php?a=hello, надрукує "hello" при включених register_globals. Якщо програміст не стежить за початковою ініціалізацією змінних, може виникнути вразливість. Ілюструється це простим прикладом:

```
if ($login == 'admin' && $password == 'пароль адміна') $is_admin = true;
.....
if ($is_admin) {
  //якісь дії, дозволені тільки адміну
}
```

Недосвідченому програмісту може здатися, що без знання пароля адміна не можна встановити змінну $is_admin в true, вона залишиться невизначеною, і if ($is_admin) не виконається. Але змінна $is_admin може бути встановлена і шляхом виклику наведеного вище скрипта з аргументом: $is_admin = 1.

Контролювати такі ситуації легше, якщо включити в PHP відображення всіх помилок, попереджень (warnings) і зауважень (notices) директивою error_reporting.

SQL-ін'єкції

Атаки SQL-ін'єкціями можливі проти сайтів, які не використовують правильне розділення SQL-запитів і вставляємих в них даних. Пояснити суть SQL-ін'єкцій найкраще на прикладі. Нехай є дошка оголошень, на ній реєструються користувачі, їм дозволено через інтерфейс видаляти свої записи. Ось код PHP-скрипта:

mysql_query ('DELETE FROM messages WHERE id =\'. $message_id. 'AND user_id =\'.$ user_id);

Змінна message_id приходить від посилання "Видалити" ($_REQUEST ['message_id']), в ній міститься ідентифікатор видаляємого запису (ціле число); змінна user_id зберігається у сесії, в неї записується ідентифікатор користувача при його успішній авторизації на сайті. Тепер припустимо, що хакер підробив адресу посилання для видалення і замість <? Message_id = 15> відправив <? Message_id = 15 OR 1 = 1>. Після підстановки цього значення в запит він стане таким:

DELETE FROM messages WHERE id = 15 OR 1 = 1 AND user_id = 3

Тут видно, що дані стали виразом, у вираз потрапило логічне "або" (OR), в результаті чого хакер "вимикає" перевірку user_id і може видаляти чужі записи. Таким чином за допомогою SQL-ін'єкції можливо видалити всі записи із бази даних. Захистом від SQL-ін'єкції можуть бути регулярні вирази. Потрібно перевіряти кожний параметр, який передається від користувача.

Міжсайтовий скриптинг XSS

XSS (Cross Site Scripting, "міжсайтовий скриптинг", названий XSS, щоб не було плутанини з CSS, таблицями стилів) являє собою атаку, при якій зловмисник публікує на атакуємому сайті скрипт (наприклад, на мові JavaScript), який виконується у користувачів сайту при відкритті ними сторінок. Оскільки цей скрипт виконується в браузері у користувача, то він має доступ до інформації в його cookie, а також може здійснювати на сайті дії від імені користувача, наприклад, читати, писати і видаляти повідомлення. Основним способом протидії XSS-атак є фільтрація прийшовших ззовні та публікуємих на сайті даних. Як правило, достатньо замінювати символи "<" і ">" на "<" і ">" відповідно (php-функція htmlspecialchars), при цьому введений відвідувачем текст втрачає HTML-оформлення, а розміщені в ньому скрипти втрачають шкідливість.

Правда, не всі сайти можуть піти на таке радикальне рішення, як ігнорування HTML-розмітки. Найчастіше, все-таки треба надати користувачеві можливість якось оформляти свої повідомлення: виділяти цитати, міняти шрифти, розфарбовувати тексти різним кольором, вставляти картинки і таблички, як, наприклад, зроблено на LiveJournal. Їм доводиться розробляти і застосовувати алгоритми часткового очищення HTML.

Відправка email з сайту

Для приховування адреси поштової скриньки від спамерів часто використовується форма зворотного зв'язку, інформація з якої надходить серверному скрипту, який вже сам відправляє пошту адресату за відомою тільки скрипту адресою, наприклад, php-функцією mail. Функція mail дозволяє відправляти лист, вказуючи йому додаткові заголовки, в яких можна прописати, зокрема, адресу відправника. Отже, можна зловити дані і передати їх у функцію mail (зворотну адресу з форми в змінній $sender_email):

mail ($admin_email, 'Лист з сайту', $message, "From:". $sender_email);

Проблема в тому, що останній аргумент функції mail являє собою розділені символами переведення рядка заголовки. Здавалося б, що заголовок один - "From". Але

уявімо, що хакер написав у якості зворотної адреси такий набір символів:

hacker@site.com
Cc: email@domain.com

Не має значення, що дані введені в 2 рядки, а у формі відправки для email було однорядкове поле, що не дає писати текст у декілька рядків. Всі дані, що надходять зовні, можна підробити. Так що даний лист буде відправлено не тільки власнику веб-сайту, а й на ті email-адреси, які хакер вкаже в "Cc:" або "Bcc:" (а він їх там може вказати сотню). І ось виникне ситуація, коли через даний веб-сайт розсилають спам. Рішення захисту від даної атаки просте – забороняти відправку листів, якщо у введеній email-адресі використовуються символи переводу рядка (\ n і \ r).

Отже, головне правило безпеки веб-сайтів говорить: ті дії, які не дозволені – заборонені.

Висновок. В сучасному світі існує безліч методів для зламу веб-сайтів, тому важливо слідкувати за новітніми технологіями, новими методами зламу веб-програм тощо. Потрібно не тільки створювати зручну функціональність та гарний дизайн веб-сайтів, але й не менш дбати про їх безпеку. Безпека – є головним критерієм хорошого веб-сайту.

Список літератури

1. Виды взломов сайтов и их предотвращение [Электронный ресурс] – режим доступа: http://www.captcha.ru/articles/antihack/

2. Голышев С.В. Защита сайта с помощью .htaccess и .htpasswd [Электронный ресурс] – режим доступа: http://www.php.su/articles/?cat=apache&page=010

3. Хакер инфо | информационный блок о хакинге [Электронный ресурс] – режим доступа: http://webcoma.ru/haker/hack.html

УДК 004.491.22

Комп'ютерні віруси, їх види та технології виявлення

Павлюк Р. П., студент 4 курсу
Науковий керівник – Савеленко О. К., викладач
Кіровоградський національний технічний університет, м. Кіровоград

У загальному випадку **комп'ютерний вірус** – це невелика програма, яка приписує себе в кінець виконуваних файлів, «драйверів», або «поселяється» в завантажувальному секторі диска. А також має здатність до прихованого саморозмноження.

Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера.

З поширенням мереж та Інтернету файлові віруси все більше орієнтуються на них як на основний канал роботи.

Також розквітають соціальні технології – спам і фішинг – як засіб зараження в обхід механізмів захисту ПЗ. Спочатку на основі троянських програм, а з розвитком технологій p2p-мереж – і самостійно – набирає обертів найсучасніший вид вірусів – хробаки-ботнети.

У залежності від середовища існування віруси можна поділити на *файлові, завантажувальні* і *поліморфні*. **Файлові віруси** проникають як правило у виконавчі модулі, тобто у файли, що мають розширення COM і EXE. А також вони можуть проникати і в інші типи файлів, але, як правило, записані в таких файлах, вони ніколи не одержують управління

і, отже, втрачають здатність до розмноження.

Завантажувальні віруси проникають у завантажувальний сектор диска (Boot-сектор) або в сектор, що містить програму завантаження системного диска (Master Boot Record).

Поліморфні віруси – віруси, що модифікують свій код у заражених програмах таким чином, що два екземпляри одного й того ж вірусу можуть не збігатися ні в одному біті.

Технології, що використовуються в сучасних антивірусних програмах можна розбити на дві групи:

1. Технології сигнатурного аналізу;
2. Технологія евристичного аналізу.

Сигнатурний аналіз – метод виявлення вірусів, що полягає в перевірці наявності у файлах сигнатур вірусів.

Сигнатурний аналіз є найбільш відомим методом виявлення вірусів і використовується практично у всіх сучасних антивірусах. Для проведення перевірки антивірусу необхідний набір вірусних сигнатур, що зберігається в антивірусній базі.

Евристичний аналіз найчастіше використовується спільно з скануванням для пошуку зашифрованих і поліморфних вірусів. У більшості випадків евристичний аналіз дозволяє також виявляти й раніше невідомі віруси. У цьому випадку, швидше за все їхнє лікування буде неможливе.

Отже, з вище сказаного можна зробити висновок, що комп'ютерні віруси продовжують розвиватися разом з іншими технологіями. Але з появою нових вірусів удосконалюються методи їх пошуку та знешкодження, тому шкода від вірусів значно менша, ніж на початку їх становлення.

Список літератури:

1. Peter Szor, The art of Computer Virus Research and defense – Addison-Weslay professional, 2005 – 744 с.
2. The Giant Book of Computer Viruses – Amer Eagle Pubns Inc, 1998 – 464 с.

УДК 371.26 – 057.87 (043.2)

Захищений модуль перевірки знань студента з дисципліни «Методологія та організація наукових досліджень»

Пархоменко Ю.О., студент 4 курсу
Науковий керівник – Щербина В.П., доцент
Національний авіаційний університет, м. Київ

Бурхливий розвиток інформаційних технологій, здійснення соціально-економічних перетворень, забезпечення конкурентоздатності фахівців вимагає впровадження нових підходів до ведення навчального процесу. В наш час стала досить актуальною перевірка знань студентів швидко та якісно. Це стає можливим за допомогою цілеспрямованого і спланованого використання інформаційних технологій тестування, головною з переваг якого є можливість контролю успішності студентів засобами систем комп’ютерного тестування. Потрібний результат досягається шляхом створення програмних засобів, що містять в собі окремо розроблену базу даних з тестами з відповідного предмету та саму програму, яка і перевіряє правильність відповідей студентів. Також для зручності, захищеності та цілісності даних засобів впроваджується захист, найрозповсюдженішим з яких є пароль, за допомогою якого заходити та редагувати програмний модуль можуть тільки викладачі та його розробники.

Галузь застосування програмних модулів перевірки знань студентів почала розвиватися в XX столітті, адже стрімкого розвитку почав набирати розвиток інформаційних та комп'ютерних технологій. З одного боку це забезпечило перехід студентів на більш високий рівень навчання і взаємодії з комп'ютерами, а з іншого зручність і швидкість перевірки викладачами більшого об'єму роботи.

Мета роботи полягає у розробці захищеного модуля, який буде перевіряти знання студентів з вивчення дисципліни «Методологія та організація наукових досліджень».

Досягнення мети потребує розв'язання таких задач як: аналіз існуючих програмних засобів тестування знань студентів та методи їх захисту; дослідження інформації та розробка методичних матеріалів для тестування студентів з дисципліни «Методологія та організація наукових досліджень»; розробка алгоритму та програми захищеного модуля перевірки знань студентів.

Під захищеним модулем будемо розуміти створення такої програми, вхід в яку буде забезпечуватися за допомогою пароля задля захисту інформації від перегляду та модифікації даних студентами.

Даний програмний модуль перевірки знань студентів з дисципліни «Методологія та організація наукових досліджень» може використовуватися у вищих навчальних закладах, де існує дана дисципліна і є необхідність комп'ютеризованої перевірки знань і застосовуватися задля якіснішої і швидшої перевірки набутих знань студентів.

Новизною роботи є те, що за рахунок розробки захищеного модуля перевірки знань студентів проведено автоматизацію навчального процесу, що дозволить швидко та якісно проводити контроль знань з дисципліни «Методологія та організація наукових досліджень» полегшуючи роботу викладачів.

Програмний модуль складається з вкладки створення тестів з даної дисципліни, проходження їх, файлів з самими тестами, та папкою, де будуть зберігатися результати тестування. У вкладці «створення тестів» є вкладка «файл», де є такі операції як закрити, відкрити, зберегти; вікна вводу питань, відповідей, балів за питання, галочки, яка позначає правильну відповідь, часу на проходження тесту; вкладки «додати питання», «ще відповідь», «зберегти». У вкладці «пройти тест» потрібно вибрати файл з темою потрібних тестів з розширенням test, ввести ПІБ та пройти відповідний тест, після чого зберегти його.

Практична цінність розробленого модуля полягає в тому, що даний захищений засіб можливо використовувати в різних навчальних закладах, де присутня дана дисципліна і таким чином автоматизувати навчальний процес і покращити якість перевірки знань студентів.

УДК:004.056

Огляд технології віртуальних пасток Honeypot

Пахомов О.В., студент 5 курсу
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Основною ідеєю технології honeypot (з англ. «горщик з медом») є створення системи, яка являє собою віртуальну приманку для зловмисників. В ході свого функціонування така система навмисне піддається атаці і виконує реєстрацію і контроль всіх дій зловмисника з метою вивчення його стратегії та визначення засобів, які використовуються для здійснення атаки, що дозволяє захистити від подібних атак реальні об'єкти безпеки.

Вперше ідея віртуальної приманки була розглянута в роботах Кліффорда Столла і Біла

Чезвіка. Вони проводили аналіз дій, що виконувались злочинцями під час злому комп'ютерних систем, на основі детальних записів про ці дії. Подальше удосконалення і розширення сфери застосування даного підходу призвело до появи технології honeypot, яка передбачала розгортання спеціальних привабливих для злочинців систем, що виконували моніторинг всіх дій в атакованій системі. В останні роки галузі застосування honeypot-приманок значно розширилися. Деякі з них розгортаються просто для марнування часу і ресурсів нападників, інші – для зменшення активності спаму чи обману зловмисників, а деякі – для аналізу діяльності хакерів при зламуванні систем і виявлення сигнатур атак.

Сучасні темпи розширення мережі Інтернет, а також збільшення об'ємів цінної інформації, що зберігається і передається в глобальних і локальних мережах, провокують появу нових методів і інструментів злому комп'ютерних систем та мереж, що в свою чергу стимулює створення нових засобів захисту інформації та попередження хакерських атак. Тому метою даної статті буде загальний огляд технології віртуальних приманок honeypot, визначення переваг і недоліків даної технології та огляд класифікації honeypot-систем.

Технологія honeypot – це передусім концепція побудови системи для злому, яка визначається не конкретним програмним забезпеченням чи особливостями конфігурації, а самою метою її побудови та розгортання. Як зазначалося вище, цією метою є виявлення вторгнень і подальший аналіз проведених атак. Існує велика кількість методів реалізації віртуальних приманок – це може бути як спеціально розгорнута цілісна мережа, так і один мережевий сервіс. Якою б не була реалізація віртуальної пастки, вона повинна привертати увагу зловмисників з метою провокування нападу. Для оцінки ефективності використання даної технології необхідно виділити її переваги та недоліки.

Honeypot-системи мають наступні переваги:

- збір змістовної інформації;
- низькі системні вимоги;
- простота встановлення, налаштування та експлуатації;
- наглядність результатів функціонування.

Також, honeypot-системи мають ряд недоліків, які не дозволяють використовувати такі системи як повноцінні механізми безпеки:

- обмежена область бачення;
- можливість розкриття honeypot-системи злочинцем;
- наявність ризику злому honeypot-системи і атака реальних об'єктів безпеки.

Тим не менш, при правильному встановленні і налаштуванні системи ці недоліки виявляються несуттєвими, а використання технології honeypot дозволяє вирішити такі завдання інформаційної безпеки, як уточнення моделей загроз і порушника, виправдання витрат на систему інформаційної безпеки, відстеження методів, що використовуються порушником та визначення нових засобів впливу зловмисників.

На відміну від таких механізмів захисту, як мережеві екрани і системи виявлення вторгнень, призначенням яких є вирішення конкретних завдань стосовно безпеки в мережі, технологія honeypot представляє собою гнучкий інструмент, використання якого підвищує рівень захищеності системи в цілому. Перелік завдань, які може виконувати конкретна honeypot-система значною мірою залежить від архітектури та налаштувань системи.

При класифікації систем honeypot використовують наступні ознаки: процес встановлення та налаштування, процес підтримки, можливості по збору даних, рівень протоколювання, рівень імітації та рівень ризику. На рисунку 1 наведено всі базові ознаки класифікації honeypot-систем та їх можливі значення.

Залежно від поставлених завдань honeypot-системи поділяють на дві категорії:

- виробничі - прості у використанні, фіксують лише найнеобхіднішу інформацію і застосовуються, переважно, великими компаніями і комерційними організаціями;
- дослідницькі – набагато складніші в розгортанні і обслуговуванні, детально фіксують усю інформацію і використовуються, переважно, дослідницькими військовими чи урядовими організаціями.

Рисунок 1 – Базові ознаки класифікації honeypot-систем та їх можливі значення

Також, системи honeypot класифікують за рівнем взаємодії зі зловмисником:
- honeypot слабкої взаємодії;
- honeypot середньої взаємодії;
- honeypot сильної взаємодії.

В таблиці 1 наведено відповідні для кожного рівня взаємодії значення основних ознак за якими характеризуються honeypot-системи.

Таблиця 1 – Характеристика рівнів взаємодії honeypot-систем

Рівень взаємодії	**Встанов-лення і налаш-тування**	**Вико-ристання і підтримка**	**Збір даних**	**Рівень протоколю вання**	**Рівень імітації**	**Рівень ризику**
Слабкий	просте	просте	обмежений	низький	низький	низький
Середній	середнє	середнє	змінний	середній	середній	середній
Сильний	складне	складне	розширений	високий	високий	високий

На сьогодні існує велика кількість різних реалізацій honeypot-систем, відмінність яких полягає в розглянутих рівнях взаємодії і різних значеннях ознак класифікації. Найвідомішими є наступні: Back Officer Friendly, Honeyd та ManTrap. Розглянемо їх детальніше.

Back Officer Friendly (BOF) – один з найпростіших варіантів honeypot, який був розроблений в 1998 році М. Ранумом. Ця система функціонально проста й зрозуміла навіть для недосвідчених користувачів. BOF може бути запущений як на Unix, так і на Windows платформах з можливістю імітації таких служб: FTP, SMTP, IMAP, POP3, HTTP, TELNET, а також троянського сервісу Back Orifice – для дистанційного адміністрування комп'ютера. Завданням системи є моніторинг подій і збереження протоколу взаємодії. В системі BOF відсутня можливість детального налаштування її роботи, саме тому вона досить проста у використанні. Одна з головних переваг BOF – його доступність, оскільки даний програмний засіб є безкоштовним, але при цьому його відносять до систем слабкої взаємодії.

Honeyd – програмний засіб, що був розроблений Н. Провасом і вперше випущений у квітні 2002 року. Honeyd є виробничою honeypot-системою з відкритим кодом для Unix платформ. Основним призначення системи є виявлення атак або несанкціонованої

активності. За рахунок того, що даний honeypot-засіб надає відкриті вихідні тексти програми, то існує можливість внутрішнього налаштування системи. Honeyd виявляє активність на всіх TCP-портах, а імітовані сервіси спроектовані тільки для введення зловмисника в оману й збору даних про його активність. Цей програмний засіб імітує систему не тільки на прикладному рівні, а й на рівні IP-стека. При цьому ймовірність успішної ідентифікації honeypot різко зменшується. Таким чином, Honeyd надає ще більший рівень обміну інформацією зі зловмисником, завдяки чому його можна віднести до honeypot-систем середнього рівня взаємодії.

ManTrap – комерційний honeypot-засіб високорівневої взаємодії, створений компанією Recourse Technologies. Унікальність ManTrap полягає в тому, що в процесі її функціонування створюється логічно контрольоване оточення, так звана пастка, з якого неможливо вийти атакуючому і реалізувати напад на реальну систему. Кожна така пастка являє собою копію повноцінної операційної системи, яка має ті ж можливості, що й справжня система, але насправді вона лише приховує в собі honeypot-систему. ManTrap надає можливість налаштування кожної пастки як реальної фізичної операційної системи. Можна створювати користувачів, робити ті, чи інші налаштування, запускати процеси, тощо. Інша корисна можливість полягає в тому, що ManTrap створює віртуальні оточення в межах однієї фізичної системи. Так, на одному комп'ютері, може бути створено до чотирьох honeypot-пасток високорівневої взаємодії. Проте, ManTrap має і деякі обмеження, основним з яких є те, що цей засіб не імітує системи, а використовує технологію пасток, тому при створенні на одному комп’ютері кількох пасток, як основа для них буде використовуватися одна реальна операційна система, що встановлена на даному комп’ютері.

Отже, honeypot являє собою ефективну та гнучку технологію, яка хоч і не може використовуватися як повноцінний засіб захисту системи, але при цьому значною мірою підвищує рівень захищеності системи в цілому. Системи, побудовані на базі технології honeypot, мають здатність ефективно працювати в мережі, збираючи невеликі об’єми інформації, при цьому значна частина цієї інформації має велику цінність при розробці заходів та методів протидії атакам зловмисників. Проте системи віртуальних приманок мають і деякі недоліки, такі як обмежена область бачення загроз та можливість їх розкриття зловмисником. Honeypot-системи можуть застосовуватися як у виробничій сфері, виконуючи такі функції як попередження, виявлення і реакція, так і бути одним з інструментів дослідження для виявлення нових методів, засобів і мотивацій зловмисників.

Список літератури

1. Гнатюк С.О., Волянська В.В., Карпенко С.В. Сучасні системи віртуальних приманок на основі технології Honeypot. – Науково-технічний журнал «Захист інформації», 2012, №3, с. 107-115.

2. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос, 2001. – 264 с.: ил.

3. Платонов В.В. Программно-аппаратные средства защиты информации. – М.: Издательский центр «Академия», 2013. – 336 с.

4. Тарасенко А. «Технология Honeypot. Часть 1-3» [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/analytics/275420.php

Напрямок 3.
Безпека інформації у хмарних сховищах

УДК 004.738.5:004.77

Система моніторингу та статистики віддалених Web-ресурсів

Висоцький С.В., студент 5 курсу,
Папуша І.П., студент 5 курсу
Науковий керівник – Бабенко В.Г., канд. техн. наук, доцент
Черкаський державний технологічний університет, м. Черкаси

Система моніторингу та статистики віддалених ресурсів представляє собою сервіс, який виконує функцію збору інформації про користувачів Інтернет ресурсів, власники яких встановили код розробленої системи до себе на Web-сторінки. Також дана система дозволяє здійснювати більш захищену аутентифікацію користувачів.

Головна відмінність створеної нами системи від вже існуючих це те, що вся інформація, яка відправляється на сервер, збирається не під час побудови сторінки браузером, як зараз роблять більшість існуючих сервісів, а після повного завантаження Web-документу. Всі дії по збереженню даних про користувача та відправка їх на сервер відбувається в фоновому режимі. Це дає можливість власникам Web-сайтів не лише значно збільшити швидкість завантаження, але й отримати при цьому повну інформацію про відвідуваність ресурсу.

Створений нами сервіс працює наступним чином: після повного завантаження сторінки користувачем, доданий на сторінку JS-скрипт отримує дані про користувача (інформацію про місце, звідки користувач прийшов на сайт; інформацію про сторінку, на якій знаходиться користувач в даний момент та інше), виконує кроссдоменний AJAX запит до сервісу та завершує роботу. Сервер після отримання даної інформації зберігає її до БД. Адміністратор сайту може отримати потрібну інформацію наступними способами:

- за домопогою WEB-інтерфейсу сервісу, де відображається повна інформація про відвідування;
- за допомогою API функцій, де адміністратор ресурсу може в online режимі отримувати дані про поточну статистику або про статистику за весь період роботи сайту (використовується принцип хмарних обчислень).

Розглянемо реалізовані принципи захисту інформації в розробленій системі моніторингу та статистики віддалених Web-ресурсів. Після відправки інформації про користувача на сервері виконується обробка вхідних даних. Вхідні дані містять в собі інформацію, яка зібрана за допомогою встановленого на сторінці скрипту, а також технічні дані, які необхідні для ідентифікації Web-сайту та користувача, а саме:

- IP-адреса користувача, який перейшов на ресурс;
- інформація про доменне ім'я сайту;
- інформація про IP-адресу сайту, на якому встановлений код.

Сервер виконує перевірку домену, з якого прийшов запит. Якщо даний домен є в базі сервісу, тобто адміністратор був раніше зареєстрований, та IP-адреса Web-сайту є в списку дозволених для даного домена (адміністратор після реєстрації додає IP-адресу чи діапазон

адрес до створеного облікового запису) – виконується збереження інформації. При використанні API функцій використовується аналогічний механізм аутентифікації користувача.

Список літератури
1. Скрембей Д. Безпека Web-додатків / Д. Скрембей, М. Шема. – К.: Вільямс, 2003. – 384 с.
2. Клементьев І. П. Введення в хмарні обчислення / І. П. Клеменьев, В. А. Устинов. – К. 2009. – 233 с.

УДК 004.75

Облачные хранилища. Защита данных: проблемы и решения

Куницкая С.Ю., канд. техн. наук, доцент,
Шкребтий А.В., студент 4 курса
Черкасский государственный технологический университет, г. Черкассы

Облачное хранилище данных (англ. *cloud storage*) — модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной. В отличие от модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту, в общем случае, не видна. Данные хранятся и обрабатываются в так называемом *облаке*, которое представляет собой, с точки зрения клиента, один большой виртуальный сервер. Физически же такие серверы могут располагаться удалённо друг от друга географически, вплоть до расположения на разных континентах.

Существующие угрозы данным в облаках

1. Традиционные атаки на ПО.

Уязвимости операционных систем, модульных компонентов, сетевых протоколов и др. — традиционные угрозы, для защиты от которых достаточно установить межсетевой экран, firewall, антивирус, IPS и другие компоненты, решающие данную проблему. При этом важно, чтобы данные средства защиты эффективно работали в условиях виртуализации.

2. Функциональные атаки на элементы облака.

Этот тип атак связан с многослойностью облака, общим принципом безопасности. Для защиты от функциональных атак для каждой части облака необходимо использовать следующие средства защиты: для прокси – эффективную защиту от DoS-атак, для веб-сервера — контроль целостности страниц, для сервера приложений — экран уровня приложений, для СУБД — защиту от SQL-инъекций, для системы хранения данных – правильные бэкапы (резервное копирование), разграничение доступа. В отдельности каждые из этих защитных механизмов уже созданы, но они не собраны вместе для комплексной защиты облака, поэтому задачу по интеграции их в единую систему нужно решать во время создания облака.

3. Атаки на клиента.

Большинство пользователей подключаются к облаку, используя браузер. Здесь рассматриваются такие атаки, как Cross Site Scripting, «угон» паролей, перехваты веб-сессий, «человек посредине» и многие другие. Единственная защита от данного вида атак является правильная аутентификация и использование шифрованного соединения (SSL) с взаимной аутентификацией. Однако, данные средства защиты не очень удобны и очень расточительны для создателей облаков. В этой отрасли информационной безопасности есть еще множество

нерешенных задач.

4. Атаки на гипервизор.

Гипервизор является одним из ключевых элементов виртуальной системы. Основной его функцией является разделение ресурсов между виртуальными машинами. Атака на гипервизор может привести к тому, что одна виртуальная машина сможет получить доступ к памяти и ресурсам другой. Также она сможет перехватывать сетевой трафик, отбирать физические ресурсы и даже вытеснить виртуальную машину с сервера. В качестве стандартных методов защиты рекомендуется применять специализированные продукты для виртуальных сред, интеграцию хост-серверов со службой каталога Active Directory, использование политик сложности и устаревания паролей, а также стандартизацию процедур доступа к управляющим средствам хост-сервера, применять встроенный брандмауэр хоста виртуализации. Также возможно отключение таких часто неиспользуемых служб как, например, веб-доступ к серверу виртуализации.

5. Атаки на системы управления.

Большое количество виртуальных машин, используемых в облаках, требует наличие систем управления, способных надёжно контролировать создание, перенос и утилизацию виртуальных машин. Вмешательство в систему управления может привести к появлению виртуальных машин — невидимок, способных блокировать одни виртуальные машины и подставлять другие.

Решения по защите от угроз безопасности

● Сохранность данных. Шифрование.

Сохраняя данные на нескольких облаках, можно существенно повысить их доступность и сохранность. Под сохранностью имеется ввиду, что данные будут существовать, даже если у одного провайдера (или нескольких) случилась серьёзная проблема. Для этого будет использоваться избыточность информации, и актуальным методом её создания сейчас является относительно новый *метод «Стирания кодов (erasure codes)»*

Суть *метода «Стирания кодов»* заключается в том, что после кодирования некоторого файла получается n фрагментов (в практической реализации это также файлы). Любые *m* из этих фрагментов равны по размеру оригинальному файлу. При этом $n > m$. Каждый из фрагментов сохраняется в отдельном облачном хранилище. Для восстановления первоначального файла достаточно собрать *m* любых фрагментов и декодировать. Остальные n-m фрагменты могут быть удалены, испорчены, содержащие их облачные хранилища не доступны и т.д. Таким образом, система использующая erasure codes может справиться с появлением $n — m$ ошибок. Соотношение параметров *n* и *m* можно выбирать.

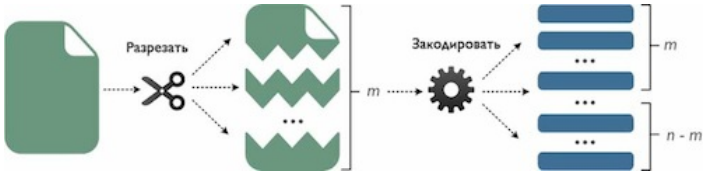

Рисунок 1 – Реализация метода MDS Erasure codes

● Защита данных при передаче.

Кроме самостоятельной защиты своих данных, при передаче на облачные сервера, используется защита предоставленная хранилищем. Разные хранилища используют свои персональные алгоритмы защиты, но самым производительным является *кодирование Рида-Соломона*. Кодирование данных происходит поэтапно, то есть в тот момент, когда один блок данных кодируется, предыдущий уже загружается на облачные хранилища. Это позволяет сократить время ожидания для пользователя.

Кодирование с помощью *кода Рида-Соломона* может быть реализовано двумя способами:

- *систематическим;*
- *несистематическим*.

При *несистематическом кодировании* информационное слово умножается на некий неприводимый полином в поле Галуа. Полученное закодированное слово полностью отличается от исходного и для извлечения информационного слова нужно выполнить операцию декодирования и только потом можно проверить данные на содержание ошибок. Такое кодирование требует большие затраты ресурсов только на извлечение информационных данных, при этом они могут быть без ошибок.

При *систематическом кодировании* к информационному блоку из k символов приписываются $2t$ проверочных символов, при вычислении каждого проверочного символа используются все k символов исходного блока. В этом случае нет затрат ресурсов при извлечении исходного блока, если информационное слово не содержит ошибок, но кодировщик/декодировщик должен выполнить $k(n-k)$ операций сложения и умножения для генерации проверочных символов. Кроме того, так как все операции проводятся в поле Галуа, то сами операции кодирования/декодирования требуют много ресурсов и времени. Быстрый алгоритм декодирования, основанный на быстром преобразовании Фурье, выполняется за время порядка $O(ln(n)^2)$.

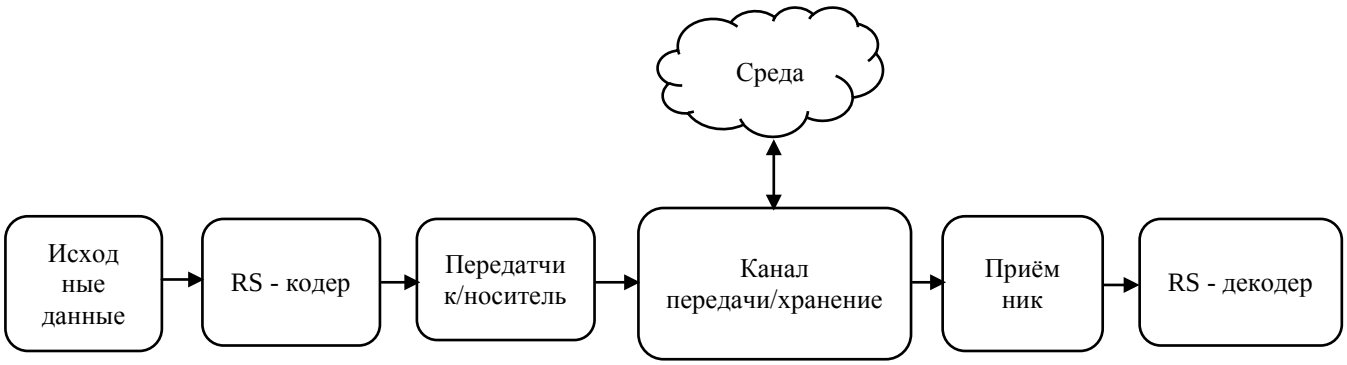

Рисунок 2 – Схема применения кода Рида-Соломона

● Аутентификация.

Аутентификации — защита паролем. Для обеспечения более высокой надёжности, часто прибегают к таким средствам, как токены и сертификаты. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации, также рекомендуется использовать LDAP (Lightweight Directory Access Protocol) и SAML (Security Assertion Markup Language).

● Изоляция пользователей.

Использование индивидуальной виртуальной машины и виртуальной сети. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service). Часто провайдеры изолируют данные пользователей друг от друга за счёт изменения данных кода в единой программной среде. Данный подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющему получить доступ к данным. В случае возможной ошибки в коде пользователь может получить иные данные.

Список использованной литературы

1. Ивонин П.В. Безопасность в облаках в деталях // Безопасность информационных технологий. – 2013. – № 2. – С. 37-40

2. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / пер. с англ. В. Б. Афанасьева. — М.: Техносфера, 2006.

3. Erasure codes – (Widipedia) http://en.wikipedia.org/wiki/Erasure_code

4. Код Рида-Соломона (Википедия) https://ru.wikipedia.org/wiki/Код_Рида_—_Соломона

УДК 004.056

Дослідження загроз для віртуальної інфраструктури хмари та методи її захисту

Ладигіна О.А., асистент
Кіровоградський національний технічний університет, м. Кіровоград

На даний час дата-центри наступного покоління розмивають кордони між фізичними та віртуальними середовищами, між публічними і приватними хмарами, що призводить до розширення ряду питань щодо захисту інформації в хмарних обчисленнях і для вирішення яких потрібні постійно удосконалючі рішення [1].

Забезпечення фізичної безпеки лежить на основі суворого контролю фізичного доступу до серверів та мережевої інфраструктури. Мережева безпека заснована на побудові надійної моделі загроз, що враховує захист від вторгнень і міжмережевий екран, з метою розмежування внутрішніх мереж дата-центрів на підмережі з різним рівнем довіри.

У хмарних обчисленнях технологія віртуалізації відіграє особливу роль і полягає в:

- віртуалізації серверів - перенесення фізичних серверів у віртуальні машини однієї хостової системи, оснащеної гіпервізором - засобом віртуалізації;

- віртуалізації робочих користувальницьких місць - централізоване зберігання робочих місць у вигляді віртуальних машин на хостовій системі з наданням роздільного доступу по мережі з фізичних робочих місць;

- віртуалізації терміналів - для окремого користувача терміналу в операційній системі створюється власний сеанс роботи.

Концепція хмарних технологій полягає в наданні користувачам віддаленого динамічного доступу до послуг, обчислювальних ресурсів і додатків, включаючи операційні системи та інфраструктуру через різні канали доступу, в тому числі і через Інтернет. Така великомасштабна інфраструктура являє підвищені ризики і досить обмежену можливість контролю над її ресурсами. У цьому і полягає актуальність проблем хмарних обчислень - захист інформації та довірливе ставлення користувачів до хмарних провайдерів.

Застосування спеціалізованого програмного забезпечення для віртуального середовища вимагає значної зміни у підходах до забезпечення інформаційної безпеки хмарних систем [2].

Рішення задач забезпечення безпеки об'єднує в собі традиційні та специфічні рішення з особливостями, які в процесі виконання задач повинні оптимізовуватись для економії продуктивності віртуального середовища із забезпеченням захисту інформації і хмарних ресурсів.

Для забезпечення безпеки і збереження цілісності даних досліджуються актуальні загрози для віртуальної інфраструктури хмари [3, 4]:

- відсутність контролю внутрішньомережевого трафіку, а також можливість прослуховування всього трафіку між віртуальними машинами;

- єдине сховище віртуальних машин, над якими можна отримати несанкціонований контроль;

- захоплення всіх ресурсів хоста віртуалізації однією віртуальною машиною, в результаті якого інші віртуальні машини можуть викликати відмову в обслуговуванні;

- незахищеність вразливих місць дискової підсистеми віртуальних машин;

- компрометація клієнтських терміналів і атака на браузери клієнтів;

- несанкціонований доступ до ресурсів віртуалізації через гіпервізор з віртуального чи

реального середовища;

- перехоплення аутентифікаційних даних для доступу до хмари через хмарні API;
- несанкціонований доступ до консолі управління віртуальним середовищем;
- відсутність у віртуальній інфраструктурі розподілених комутаторів, які при міграції віртуальних машин дозволяють погоджувати політику безпеки;
- перехоплення даних при передачі по незахищених зовнішніх каналах зв'язку.

Одним з головних джерел загрози безпеки є сервер централізованого управління віртуальної інфраструктури, отримавши контроль над яким, зловмисник отримує повний доступ до всіх віртуальних машин, хостів віртуалізації, віртуальних мереж і сховищ даних.

Тому необхідно, в першу чергу, ретельно захищати сам сервер управління, звертати посилену увагу на засоби аутентифікації і розмежування прав доступу, для чого має сенс використовувати додаткове програмне забезпечення, що розроблене спеціально для віртуальних інфраструктур. Доступ до сервера віртуалізації повинен здійснюватися за безпечними протоколами, а доступ адміністраторів повинен бути обмежений за IP-адресами.

Важливо також, щоб мережі управління віртуальною інфраструктурою та виробничого середовища віртуальних машин були розділені логічно і фізично для запобігання несанкціонованого втручання.

При дослідженні загроз ще слід враховувати також специфіку обробки персональних даних у віртуальному середовищі [5, 6]:

- обробляються в рамках віртуальних машин;
- передаються між віртуальними машинами всередині віртуального середовища;
- передаються між віртуальним середовищем і зовнішніми середовищами, як реального, так і віртуального.

Для забезпечення захисту даних у хмарі, які розміщені за межами сфери фізичного доступу клієнта, здійснюють шифрування віртуальних жорстких дисків. При зчитуванні з диска дані розшифровуються і при записі на диск зашифровуються. При цьому ключі зберігаються на окремому сервері управління ключами, який спочатку перевіряє ідентифікаційні дані і цілісність хмарного сервера, який направив запит. У разі позитивного відгуку надається ключ і хмарний сервер отримує доступ до інформації, що зберігається і ресурсів хмари.

Більш потужний варіант безпеки даних являє собою комбінування технологій шифрування даних і захищеної передачі.

Для підвищення безпечного використання хмарних технологій доцільно використовувати системи виявлення вторгнень і міжмережевого екранування з контролем зовнішніх підключень до середовища віртуалізації за допомогою апаратних рішень, а внутрішніх - за допомогою програмних рішень, реалізуючи, таким чином, комбінований підхід.

Швидко виявити атаки зловмисника дозволяють журнальні записи, зроблені серверами хмари, які служать важливим джерелом інформації при проведенні інженерно-технічних експертиз. Тому збереження журнальних записів за весь термін служби хмарного сервера є важливою, необхідною мірою і дозволить здійснити подальший аналіз збору даних, їх об'єднання та виведення на зовнішні інструменти, платформу безпеки або на систему управління подіями інформаційної безпеки.

Наступними ефективними засобами захисту хмар є:

- довірене завантаження серверів віртуалізації, віртуальної машини, серверів управління віртуалізацією;
- сегментування віртуальної інфраструктури для обробки персональних даних користувачем або групою користувачів;
- ідентифікація та аутентифікація доступу та об'єктів доступу у віртуальній інфраструктурі, в тому числі адміністраторів управління засобами віртуалізації;
- управління доступом суб'єктів доступу до об'єктів доступу у віртуальній інфраструктурі, в тому числі всередині віртуальних машин;

- управління потоками інформації між компонентами віртуальної інфраструктури, а також по периметру віртуальної інфраструктури.

Для антивірусного захисту віртуальних машин краще використовувати безагентний підхід, що забезпечує комплексну безпеку без установки агентського модуля в захищаємій системі, тобто у віртуальне середовище впроваджується віртуальний пристрій - шлюз безпеки, який бере на себе функції антивіруса для всіх віртуальних машин.

Вірно підібрані рішення безпеки дозволяють отримати уявлення про рівень використовуваних ресурсів і своєчасно виявити атаки, які націлені на різні хмарні об'єкти.

Для зниження операційних витрат, пов'язаних із засобами захисту систем віртуалізації, рекомендується використовувати спеціально розроблене програмне забезпечення, що адаптоване для хмарних обчислень.

Але все ж ще залишаються проблеми адаптації захисту віртуалізації в хмарі, які вимагають подальшого аналізу і вдосконаленого рішення.

Список літератури:

1. Котяшичев И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности / И. А. Котяшичев, Е. А. Бырылова // Молодой ученый. — 2015. — №6.4. — С. 30-34.

2. Ладигіна О.А. Перспективи захисту інформації в хмарних обчисленнях від атак на засоби віртуалізації // Збірник тез доповідей науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія».- Кіровоград: КНТУ, 2014. -164 с

3. Ширманов А. Безопасность виртуализации при обработке данных ограниченного доступа // Москва, ЭКСПОЦЕНТР, InfoSecurity Russia. 30 сентября 2009

4. Е. Кожемяка Обеспечение безопасности данных при использовании облачных технологий/ [Електронний ресурс]. – Режим доступу: http://www.lastmile.su/files/article_pdf/3/article_3823_334.pdf

5. Котяшичев И. А. К вопросу о безопасности облачных технологий в информационной среде/ И. А. Котяшичев, С. В. Смоленцев // Молодой ученый. — 2014. — №5.1. — С. 25-28.

6. Бойко А., Бердник А. Методы защиты виртуальной среды. Программный комплекс для проведения автоматизированного аудита виртуальной среды на предмет наличия ошибок в конфигурации безопасности/ [Електронний ресурс]. – Режим доступу: http://cyberleninka.ru/article/n/metody-zaschity-virtualnoy-sredy-programmnyy-kompleks-dlya-provedeniya-avtomatizirovannogo-audita-virtualnoy-sredy-na-predmet

УДК 004.75:378.147

Аналіз безпеки даних в хмарних сервісах

Ліщина Н.М., канд. техн. наук, доцент
Луцький національний технічний університет, м. Луцьк

Хмарні технології визначають як динамічно масштабований вільний спосіб доступу до зовнішніх обчислювальних інформаційних ресурсів у вигляді сервісів, що надаються за допомогою мережі Інтернет.

Хмарні технології дозволяють споживачам використовувати програми без установки і доступу до особистих файлів з будь-якого комп'ютера, що має доступ в Інтернет. Ця технологія дозволяє вести значно ефективніше управління підприємством за рахунок централізації управлінської та облікової інформації, обробки, пропускної здатності та надійності зберігання даних.

Головним стримуючим фактором при роботі з «хмарними» ресурсами є питання безпеки – відсутність контролю над серверами, обчислювальними процесами, можливість витоку критично важливої інформації. Серед інших стримуючих факторів можна відзначити сумніви в якості «хмарних» послуг, незначна кількість пропозицій, відсутність методик оцінки ефективності, неготовність змінювати підходи до IT-стратегій, неприйняття IT-

персоналом, нерозуміння керівниками компаній переваг нових технологій.

Насамперед згадані побоювання справедливі у випадку банків та інших фінансових установ, що є об'єктом дуже жорсткого контролю з боку державних регуляторних органів. А для вирішення багатьох завдань (таких, наприклад, як внутрішня бухгалтерія, CRM, HR та ін) фінансові організації цілком можуть використовувати «хмарні» обчислення вже сьогодні. З провайдером «хмарних» обчислень можна підписати відповідний договір про рівень обслуговування (SLA), що передбачає серйозні фінансові штрафні санкції у випадку тих чи інших небажаних подій.

Фахівці провідних світових IT-компаній вважають, що дані, які поміщені в «хмару», надійно захищені і у віртуальній, і у фізичній реальності, оскільки величезні ЦОД з серверами, на яких зберігаються терабайти інформації, забезпечують найвищий рівень захисту від зловмисників, природних катаклізмів та інших зовнішніх загроз.

Найбільш відомими у світі є безкоштовні хмарні платформи Microsoft Office 365, Google Apps Education Edition та хмарні сервіси на їх основі. Розглянемо організацію безпеки даних в Office 365 .

Office 365 – це надійно захищена служба, розроблена відповідно до життєвого циклу розробки систем безпеки Microsoft. Це інтегроване рішення "програмне забезпечення як послуга", об'єднує практичний досвід, накопичений за два десятиліття розробки корпоративного програмного забезпечення та керування онлайновими службами. На рівні послуги в Office 365 використовується підхід поглибленого захисту, який передбачає кілька шарів функцій безпеки та передових практик (фізичний шар, логічний шар і шар даних). Крім того, служба Office 365 надає засоби керування корпоративного класу для користувачів і адміністраторів, за допомогою яких можна додатково посилити захист свого середовища.

Коли ви довіряєте свої дані службі Office 365, ви залишаєтеся їхнім єдиним власником – ви зберігаєте всі права власності та інші речові права на дані, які зберігаються в Office 365. Згідно з політикою Office 365 дані можуть бути використані лише з метою, пов'язаною з наданням послуг, а не в рекламних цілях. [2]

Засоби керування конфіденційністю дають змогу контролювати доступ до даних, надаючи його лише певним особам у вашій організації. Спеціальні конструктивні елементи запобігають змішуванню даних з інформацією інших організацій, які використовують Office 365. Масштабні перевірки та строгий нагляд запобігають несанкціонованому доступу адміністраторів до даних.

Фізична безпека гарантує: цілодобовий контроль центрів обробки даних; багатофакторну аутентифікація, зокрема біометричне сканування, для доступу до центрів обробки даних; внутрішню мережу центру обробки даних, відділену від зовнішньої мережі; поділ за ролями, завдяки якому персонал, що має фізичний доступ до місця зберігання даних, жодним чином не може визначити розташування конкретних даних клієнтів; розмагнічування та знищення несправних дисків і устаткування.

Логічна безпека включає: багаторівневу схему розмежування для строго контрольованого процесу ескалації, що суттєво обмежує доступ людей до ваших даних; виконання на серверах лише процесів зі списку дозволених для мінімізації ризиків, пов'язаних із виконанням зловмисного коду; спеціальні групи, що відповідають за керування загрозами та активно прогнозують спроби зловмисників отримати доступ до даних, запобігають таким спробам і пом'якшують наслідки, якщо вони виявляються вдалими; сканування портів, пошук вразливостей по периметру та виявлення вторгнень, що дають змогу запобігти доступу зловмисників або виявити такий доступ.

Безпека даних дозволяє: зберігання даних на віддалених серверах у зашифрованому вигляді; шифрування даних за допомогою технології SSL або TLS перед їх передаванням між вами та корпорацію Майкрософт; керування загрозами, моніторинг стану безпеки та перевірка цілісності файлів або даних для запобігання будь-яким спробам несанкціонованого доступу до даних або виявлення таких спроб.

У службі Microsoft Office 365 адміністратор має у своєму розпорядженні багато

засобів, що допомагають ефективно керувати електронним зв'язком у навчальному закладі та здійснювати над ним контроль.

Закритий фільтр навчального закладу — дозволяє обмежити зв'язок доменом.

Фільтр брандмауера на етичній основі — надає можливість запобігти спілкуванню з допомогою електронної пошти між двома попередньо визначеними особами або групами.

Фільтр непристойних слів — дозволяє блокувати повідомлення електронної пошти, які містять непристойні слова, включені до попередньо складеного списку.

Служба Microsoft Office 365 містить широкий набір функцій захисту конфіденційності та не сканує електронну пошту або документи в рекламних цілях. Завдяки постійному резервному копіюванню даних, можливостям аварійного відновлення та розташованим по всьому світу центрам обробки даних ваші документи та служби будуть доступні 24 години на добу і 7 днів на тиждень.[1]

Для забезпечення безпеки інформації, хмарні обчислення надають такі переваги:

– спеціалізований персонал: провайдер хмари, як велика організація, для забезпечення безпеки в хмарі наймає спеціалістів у галузі безпеки інформації, що дозволяє співробітникам зосередитися виключно на питанні безпеки, досягти високого рівня безпеки, якого неможливо досягти в невеликій організації;

– централізоване керування, конфігурація системи безпеки та її аудит;

– стійкість платформи: апаратний та програмний склад платформи, на якій розгорнуто хмару більш рівномірно, ніж у більшості традиційних обчислювальних центрів, що дозволяє краще автоматизувати діяльність щодо забезпечення безпеки, тестування та виправлення помилок у компонентах платформи;

– наявність ресурсів: можливість динамічного масштабування ресурсів системи, а також резервування та аварійного відновлення, що може бути використано для підвищення стійкості системи проти атак типу «відмова в обслуговуванні», а також швидкого відновлення після серйозних інцидентів;

– резервне копіювання і відновлення: провайдер хмарних послуг може дозволити надання більш високого рівня резервного копіювання і відновлення, ніж той, що забезпечують традиційні центри обробки даних, а також забезпечити зберігання резервних копій за географічною вимогою;

– мобільність кінцевих клієнтів: завдяки архітектурі хмари клієнти можуть використовувати різноманітні портативні пристрої, з невеликою обчислювальною потужністю, виходом до мережі Інтернет, браузером та/або декількома встановленими додатками, щоб отримати доступ до основних обчислювальних ресурсів;

– концентрація даних: використання хмари, як єдиного місця для зберігання та обробки даних, у деяких випадках дозволяє підвищити безпеку, ніж зберігання даних, що розосереджені по портативних комп'ютерах, вбудованих пристроях або зберігаються на знімному носії. [3]

Список літератури

1. Морзе Н. Хмарні обчислення в освіті: досвід та перспективи впровадження / Морзе Н., Кузьмінська О. // Інформатика. – 2012. — №1. — 109 с.

2. Office 365 для навчальних закладів [Електронний ресурс]. — Режим доступу: http://www.microsoft.com/uk"ua/office365/edu" cation/compare"plans.aspx.

3. Яковицький І.Л. Технологія «Хмарних обчислень» як інструмент створення інформаційної інфраструктури управління. [Електронний ресурс]. — Режим доступу: http://www.nbuv.gov.ua/ portal/soc_gum/kg.

УДК 004.49.5

Метод управления доступом к «облачным» ресурсам для защиты телекоммуникационных систем

Смирнов А.А., д-р техн. наук, профессор,
Мохамад Абу Таам Гани, аспирант,
Смирнов С.А., аспирант
Кировоградский национальный технический университет, Кировоград

У пользователей в современных информационно-телекоммуникационных системах все большим спросом пользуются услуги облачных антивирусных систем. Связано это во многом с одной стороны с динамическим развитием сетевых технологий, а с другой, ростом реальных угроз зловредного программного обеспечения, справиться с которым стационарные антивирусные системы не в состоянии. Облачные антивирусы являются комплексами из клиентского приложения и веб-сервиса. Обе части антивируса работают совместно. Клиент – это небольшая программа, которая работает на компьютере пользователя и сканирует систему, проверяя, не заражена ли она вредоносным кодом. Известно, что традиционные антивирусные программы, устанавливаемые на компьютер, являются «пожирателями ресурсов», но клиентские программы облачных антивирусов требуют намного меньше вычислительной мощности [1-6]. Веб-сервис облачного антивируса располагается в Интернете, на одном или нескольких серверах. Большую часть задач по обработке данных выполняет именно он, поэтому компьютеру пользователя не приходится ни обрабатывать, ни хранить значительные объемы информации. Через определенные промежутки времени программа-клиент сканирует компьютер. Суть сканирования состоит в поиске вредоносного кода, информация о котором есть в базе данных веб-сервиса [1-6].

Теперь перечислим те преимущества, которыми обладает облачный антивирус в сравнении с традиционным [1-6]:

– Программа-клиент имеет доступ к самым свежим данным о вредоносном коде спустя всего несколько минут после того, как о нем «узнал» веб-сервис. Нет необходимости постоянно обновлять антивирусное программное обеспечение.

– Программа-клиент очень мала и довольствуется небольшой вычислительной мощностью. Следовательно, она не отвлекает компьютер от других выполняемых им задач.

– Облачные антивирусы бесплатны. Впрочем, обновления, дополнительные утилиты и поддержка предлагаются за деньги.

Теперь, когда мы узнали о том, что представляет собою облачное антивирусное программное обеспечение, рассмотрим те функции, которые выполняет типичный облачный антивирус [1-6]. Интерфейс пользователя облачного антивируса не вызовет серьезных вопросов ни у кого из тех, кто имеет опыт использования традиционных антивирусных программ. И работу он выполняет ту же: сканирует компьютер, выявляет вредоносный код и чистит от него систему [1-6]. Перечислим основные функции, доступные в пользовательском интерфейсе облачного антивируса [1-6]:

– Сканирование всего компьютера или отдельных папок.

– Возможность настройки автоматического режима сканирования с указанием тех файлов, которые следует включить в область сканирования.

– Просмотр подробного отчета о том, какой вредоносный код был обнаружен в процессе сканирования.

– Действия по удалению или восстановлению файлов, помещенных в карантин или файлов, которые были обезврежены тем или иным способом.

В этих основных функциях отличий от традиционного антивируса не наблюдается. Но

есть те возможности, которые свойственны исключительно облачным антивирусным сервисам. Как уже говорили, облачный антивирус распределяет выполнение своих задач между компьютером пользователя (программа-клиент) и удаленным веб-сервером (или несколькими серверами), доступ к которому осуществляется через Интернет [1-6].

Таким образом, часть ресурсов является «общей» для всех пользователей. Это не только вычислительные мощности серверов, но и центральная база данных, содержащая данные о вредоносном коде. Эта база данных составляется различными способами. Для каждого продукта характерны свои методы ее пополнения.

Облачные базы данных отличаются не только методиками сбора информации. Реальным преимуществом облачных антивирусов является та скорость, с которой они способны обеспечить защиту от новых угроз [1-6].

В облачных антивирусах предусмотрена также возможность кеширования базы данных на компьютере для дальнейшего использования в офлайн-режиме. Разумеется, в этом случае база будет содержать данные по состоянию на момент ее сохранения. Этот кеш может обновляться во время выхода компьютера в Интернет. Но он не содержит полный перечень информации о вредоносном коде, только о наиболее распространенных угрозах [1-6].

Процесс информационного обмена оконечных рабочих станций с узлами, предоставляющими услуги облачной антивирусной защиты, представляет собой четко организованную функциональную структуру, являющуюся совокупностью методов формирования сигнатур, транспортировки, коммутации, маршрутизации и обработки специализированными анализаторами.

Таким образом, актуальной научной задачей является усовершенствование метода управления доступом к соответствующим «облачным» телекоммуникационным ресурсам.

Для решения поставленной оптимизационной задачи повышения оперативности обработки информационных пакетов в интеллектуальных узлах коммутации при их передаче в «облачные» антивирусные системы предлагается разработать метод управления доступом к соответствующим «облачным» телекоммуникационным ресурсам. В основу рассматриваемого метода положена процедура вычисления виртуального времени обработки информационных пакетов, отличающаяся от известных учетом фактора введения дополнительного уровня приоритезации для информационных пакетов метаданных [7-12]. При этом указанные информационные пакеты получают наивысший приоритет обработки в интеллектуальных узлах коммутации класса r_1.

На первом шаге в предложенном методе осуществляется проверка нахождения пакетов на входе интеллектуального узла коммутации. При их отсутствии – метод переходит в режим ожидания поступающих пакетов. В случае, когда на вход интеллектуального узла коммутации информационные пакеты поступили (всех уровней приоритезации или только отдельных) необходимо выполнить выбор из каждой очереди буфера памяти интеллектуального узла коммутации по одному первому пакету $r_1 = 1$, $r_2 = \overline{2, J}$ и $r_3 = \overline{J+1, R}$ уровня приоритетности для определения «эталонного» информационного пакета с соответствующим уровнем приоритетности. Это позволит сократить время обработки информационных пакетов метаданных при обеспечении заданных показателей оперативности обработки информационных пакетов других уровней приоритетности.

На следующем шаге в рассматриваемом методе определяется значение VST (виртуального времени обработки информационных пакетов) и VFT (виртуального времени обслуживания в очереди). Далее приступаем к выполнению процедур выявления информационного пакета для обработки в обслуживающем устройстве интеллектуального узла коммутации. При этом учитывается следующее: на вход буферного устройства может поступать N пакетов (N – количество очередей в системе) r_1, r_2 и r_3 уровней приоритетности.

Если значение VST наступило, то из информационного потока выбирается первый

(«эталонный») пакет, с некоторым $N_{приор}$, а также значением VFT.

Далее производится сравнение «эталонного» информационного пакета с другими поступившими на данный момент времени. При этом процедура управления с помощью исключения в «эталоне» является отличительной особенностью рассматриваемого метода управления доступом к «облачным» телекоммуникационным ресурсам. Данные исключения необходимы для обеспечения качества обслуживания информационных пакетов других (низших) приоритетов. Информационные пакеты можно сравнивать попарно, при этом в начальный момент времени первый выбранный информационный пакет условно обладает высшим уровнем приоритетности. На следующем шаге происходит переход непосредственно к процедурам обработки информационных пакетов. После этого, информационному пакету присваиваются текущие значения VST и VFT с целью дальнейшего сопровождения информационного пакета к пункту назначения. Далее информационный пакет добавляется в выходную очередь и заканчивается процесс его обработки в интеллектуальном узле коммутации.

Таким образом, разработан метод управления доступом к «облачным» телекоммуникационным ресурсам, отличающийся от известных введением нестандартных условий принятия решения о присвоении «эталонного» приоритета информационному пакету на основе дополнительного показателя – вероятности присвоения приоритета. Это дает возможность решить задачу минимизации времени обработки информационных пакетов метаданных при их передаче в «облачные» антивирусные системы при обеспечении заданного качества обслуживания других информационно-телекоммуникационных услуг.

Список литературы

1. A. Matrosov, E. Rodionov, D. Harley “Stuxnet under microscope”. Доступен на http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

2. S. Cobb «Stuxnet, Flamer, Flame, Whatever Name: There’s just no good malware». Доступен на http://blog.eset.com/2012/06/03/stuxnet-flamer-flame-whatever-name-there-is-no-good-malware.

3. Zesheng Chen, Lixin Gao, Kevin Kwait. Modeling the spread of active worms. INFOCOM 2003. Доступен на http://www.ieee-infocom.org/2003/papers/46_03.PDF.

4. K. Rohloff , T. Basar, Stochastic Behavior of Random Constant Scanning Worms [Text] / K. Rohloff, T. Basar // Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on 17-19 Oct. 2005, pp. 339 – 344.

5. M.M. Williamson, J. Leveille Epidemiological model of virus spread and cleanup. HPL-2003-39. Доступен на http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf.

6. О.Добвня. Как работают облачные антивирусы. Доступен на http://hi-news.ru/software/fakty-kak-rabotayut-oblachnye-antivirusy.html

7. Давыдов, В.В. Сравнительный анализ моделей распространения компьютерных вирусов в автоматизированных системах управления технологическим процессом [Текст] / В.В. Давыдов // Системи обробки інформації. – Харків: ХУПС, 2012. – Вип. 3(101), Том 2. – С. 147-151.

8. Семенов, С.Г. Математическая модель распространения компьютерных вирусов в гетерогенных компьютерных сетях автоматизированных систем управления технологическим процессом [Текст] / С.Г. Семенов, В.В. Давыдов // Вісник Національного технічного університету «ХПІ». Збірник наукових праць. Серія: Інформатика та моделювання. – Харків: НТУ «ХПІ», 2012. – Вип. 38. – С. 163-171.

9. Смирнов А.А. Математическая GERT-модель технологии передачи метаданных в облачные антивирусные системы / В.В.Босько, А.А.Смирнов, И.А.Березюк, Мохамад Абу Таам Гани // Збірник наукових праць "Системи обробки інформації". – Випуск 1(117). – Х.: ХУПС – 2014. – С. 137-141.

10. Смирнов А.А. Структурно-логическая GERT-модель технологии распространения компьютерных вирусов / А.А.Смирнов, И.А.Березюк, Мохамад Абу Таам Гани // Системи управління, навігації та зв’язку. – Випуск 1(29). – П.: ПНТУ. – 2014. – С. 120-125.

11. Smirnov A.A. Experimental studies of the statistical properties of network traffic based on the BDS-statistics / A.A. Smirnov, D.A. Danilenko // *International Journal of Computational Engineering Research (IJCER).* – Volume 4, Issue 5. – India. Delhi. – 2014. – P. 41-51.

12. Смирнов А.А. Дисперсионный анализ сетевого трафика для обнаружения и предотвращения вторжений в телекоммуникационных системах и сетях / А.А. Кузнецов, А.А. Смирнов, Д.А. Даниленко // Збірник наукових праць "Системи обробки інформації". – Випуск 2(118). – Х.: ХУПС – 2014. – С. 124-133.

Напрямок 4.
Криптографічні засоби захисту інформації

УДК 004.056.55

Роль квантового комп’ютера у долі криптографії

Буравченко І.А., студент 2 курсу
Науковий керівник – Конопліцька-Слободенюк О.К., викладач
Кіровоградський національний технічний університет, м. Кіровоград

Завдання криптографії, тобто таємна передача, виникає тільки для інформації, яка потребує захисту. У таких випадках говорять, що інформація містить таємницю або захищається, є приватною, конфіденційною або секретною. Для найбільш типових ситуацій введено спеціальні поняття:

- Державна таємниця;
- Військова таємниця;
- Комерційна таємниця;
- Юридична таємниця;
- Лікарська таємниця і т. д.

Усе здавалося б добре, криптографія допомагає людям шифрувати ту інформацію, яку вони хочуть вберегти від сторонніх очей, але не все так добре. Сучасний світ багато в чому являє собою набір цифрових сервісів, надійність та безпечність яких повністю залежить від криптографії. Однак ми знаходимося на порозі цифрової революції, яка дасть нам надшвидкі обчислювальні машини – квантові комп’ютери.

Квантовий комп'ютер – фізичний обчислювальний пристрій, функціонування якого ґрунтується на принципах квантової механіки, зокрема, принципі суперпозиції та явищі квантової заплутаності. Теоретично квантовий комп'ютер здатний розв'язувати певні задачі набагато швидше, ніж звичайні комп'ютери, в тому числі і задачі криптоаналізу.

Експерти попереджають, що потужність квантових комп’ютерів може легко обходити популярні засоби шифрування. І це може стати причиною хаосу в цифровому світі та спричинити настання темних часів цифрової ери.

Мало хто замислюється, проте майже кожна передача інформації по цифрових каналах ведеться в зашифрованому вигляді. Це стосується мобільних телефонів, переказу грошей та навіть результатів пошуку. Google, наприклад, знижує рейтинг веб-ресурсів, які не використовують шифрування.

Коли якесь повідомлення захищають криптографічними методами, для його читання потрібний ключ – дуже велике число з десятків або навіть сотень розрядів. Шукати його підбором на звичайних комп’ютерах займає багато часу, оскільки потрібно перебрати мільярди варіантів та обрахувати їх через складні математичні формули.

Тому навіть суперкомп’ютери не можуть забезпечити прийнятний час розшифровування для довгих ключів. Наприклад, популярний алгоритм шифрування RSA з довжиною ключа в 768 бітів можна зламати за два роки за допомогою системи з декількох сотень комп’ютерів. Проте ті, хто користується цим шифром, вже давно перейшли на ключ довжиною 2048 бітів, а кому потрібний більший захист – впроваджують 4096 бітів.

Цій майже ідилічній картині можуть завадити квантові комп’ютери, які здатні оброблювати паралельно багато потоків інформації. Це значно скорочує потрібний час для

злому шифру, оскільки вони підбирають паролі не по одному в одиницю часу, а по декілька трильйонів.

Поки що квантові комп'ютери доступні лише великим дослідницьким корпораціям, однак з їхнім поширенням, вважають експерти, для електронної торгівлі можуть настати темні часи. Адже шифруванню вже не можна буде довіряти, і продавати речі доведеться, як у доцифрову епоху: віч-на-віч та серед кола знайомих.

Криптографія на основі публічного ключа базується на проблемах числової теорії, факторизації та дискретних логарифмів, усі з них можна легко подолати, якщо мати потужний квантовий комп'ютер.

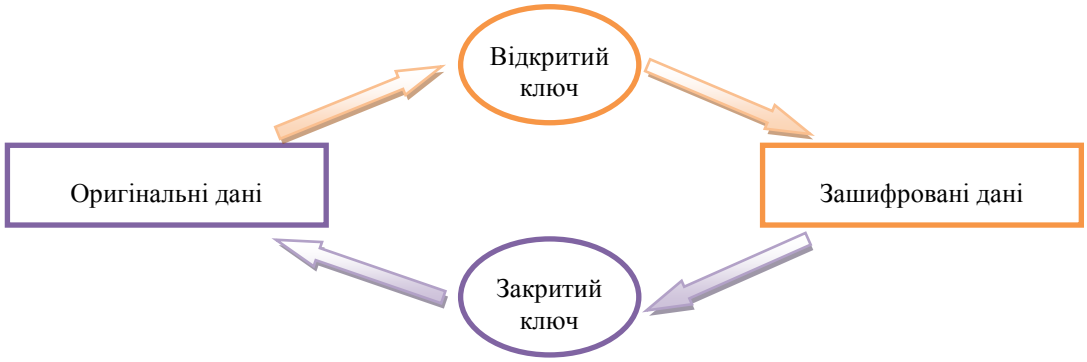

Рисунок 1 – Криптографія на основі публічного ключа

Та не все так погано, на даний час квантові комп'ютери не дуже потужні, проте вони мають потенціал. Сьогодні квантові комп'ютери знаходяться на стадії, коли навіть чітко не зрозуміло, з яких матеріалів їх потрібно виготовляти.

Окрім цього, дослідникам також необхідно прийти до єдиного стандарту архітектури кубітів, щоб їх можна було з'єднувати між собою. Сьогодні вдається об'єднати лише декілька сотень кубітів в одну машину, чого замало для практичних цілей. Існують різні пропозиції для створення кубітів, проте всі вони мають переваги та недоліки, і ще не зрозуміло, який підхід варто обрати.

Але ж квантові комп'ютери не тільки складають велику загрозу для сучасних методів криптографії, але й передують створенню нових методів криптографії, які на відміну від сучасних методів будуть набагато і набагато надійнішими.

Квантова криптографія – розділ криптології, що базується на застосуванні підходів та методів квантової механіки (зокрема, квантової передачі інформації та квантових обчислень) до проблем криптографії та криптоаналізу.

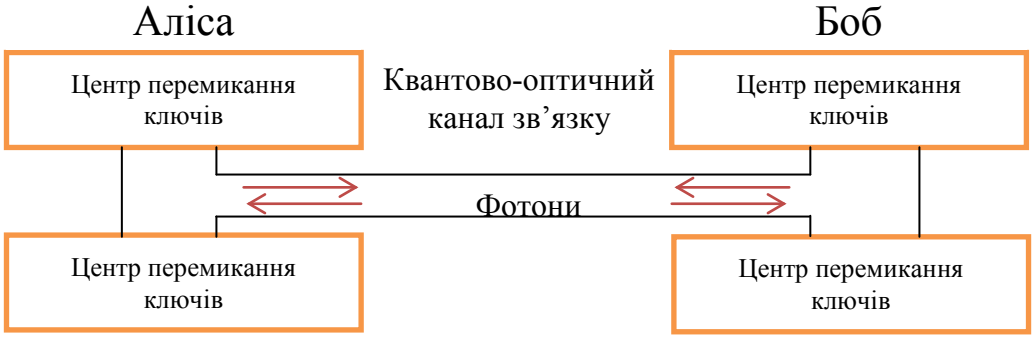

Рисунок 2 – Перша квантово-криптографічна схема

Найвідоміший та найкраще розроблений метод квантової криптографії – це квантовий розподіл ключа, який описує процес застосування квантової комунікації для створення та обміну секретним ключем між двома користувачами (яких в теорії інформації традиційно називають Алісою і Бобом) без можливості втручання третьої сторони (Єви), що прагне перехопити інформацію про ключ. При цьому Єва може навіть підслухати зв'язок між

Алісою і Бобом, але таке втручання може бути одразу виявлене. Це досягається за рахунок того, що Аліса, відправляючи повідомлення Бобові, зашифровує біти ключа як квантову інформацію. Завдяки принципам квантової механіки, навіть якщо Єва намагається перехопити ці біти, повідомлення буде збурене і міститиме помилки, які Аліса і Боб можуть виявити. Якщо ж втручання Єви не виявлене, то отриманий ключ може бути використаний для секретної комунікації.

Висновок: отже, квантові комп'ютери несуть не тільки загрозу, але й можливі покращення у області криптографії, тож остаточно, доля сучасного шифрування достовірно не визначена. Будемо сподіватися на те, що певні нововведення у сучасних технологіях, надалі будуть лише покращувати життя людини, а не ставити його під загрозу так як це було з винайденням розпаду атомних елементів.

Список літератури

1. Введення в криптографію / За заг. ред. В.В. Ященко. - 3-е вид., Доп. - М.: 2000.-288с.

2. Mark Ward Do quantum computers threaten global encryption systems? – BBC News [Електронний ресурс]. – Режим доступу: http://www.bbc.com/news/business-27974877

УДК 004.056.55

Алгоритм блочного симметричного шифрования на основе псевдопреобразования Адамара

Елисеев Р.Ю., студент 2 курса

Научный руководитель – Халимов Г.З., д-р техн. наук, профессор

Харьковский национальный университет радиоэлектроники, Харьков

Внутреннее состояние предложенного шифра представлено матрицей n*m байт, где n – количество строк (является степенью 2), а m – количество столбцов, но в дальнейшем для упрощения будет представлен частный случай с блоком 4*4 байта (128 бит). В таком режиме шифр работает подобно SQUARE [1] и AES на каждом раунде производя 4 различных обратимых преобразований: нелинейную подстановку S, байтовый сдвиг τ, псевдопреобразование Адамара над столбцами, наложение раундового ключа.

В процессе нелинейной подстановки S каждый байт блока заменяется соответствующим ему в псевдослучайной подстановке. ByteShaker использует таблицы подстановок алгоритма Anubis.

Байтовая перестановка τ выполняет функцию перемешивания столбцов матрицы состояния шифра и выполняется следующим образом: каждая i-я строка циклически сдвигается влево на 1+i байт, т.е. 1 строка сдвинется влево на 1 байт, вторая – на два, 3-я на 3, а четвертая – останется на месте.

Смешивание столбцов матрицы выполняется последовательным применением над байтами четырехточечного быстрого псевдопреобразования Адамара [2].

Четвертое преобразование – наложение раундового ключа – осуществляется наложением предварительно подготовленной ключевой информации на блок состояния с помощью поразрядной операции xor.

Все операции, используемые в алгоритме, имеют обратные (кроме xor, она является инволютивной) преобразования. При обратном криптопреобразовании операции применяются в обратном порядке.

Подготовка раундовых ключей осуществляется по следующей схеме:

- начальное заполнение «искренним числом» - мантиссой числа Пи [3];
- циклическое наложение ключа шифрования на расписание;
- первый ключ расписания остается неизменным;
- для каждого последующего элемента расписания выполнить 8 раз:
  - выполнить преобразования S и PHT предыдущего элемента расписания;
  - выполнить раунд шифрования над текущим элементом, в качестве ключа использовать предыдущий элемент.

Алгоритм имеет невысокие требования к памяти, так, ему требуется хранить 384 бита информации для 128 битного блока (128 бит для 2 таблиц подстановки 4x4 плюс текущий и следующий 128-битные раундовые ключи).

Количество раундов рассчитывается по формуле 1+lk/8, где lk – длина ключа шифрования в битах.

Список литературы

1. The Block Cipher Square Algorithm, // Joan Daemen, Lars R. Knudsen and and Vincent Rijmen, Dr. Dobb's Journal, October 01, 1997.

2. Fast Pseudo-Hadamard Transforms. // Tom St Denis

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с. – 3000 экз. – ISBN 5-89392-055-4.

УДК 004.051.(043.2)

Модифицированный алгоритм Евклида для деления больших целых чисел двойной и одинарной точности

Ковтун М.Г., аспирант

Научный руководитель – Гнатюк С.А., канд. техн. наук, доцент

Национальный авиационный университет, г. Киев

С увеличением роли информации в жизни современного общества и развитии государственных информационных ресурсов, а также переходе от классического военного противостояния к противостоянию в информационной сфере, возникает острая необходимость в защите информационных ресурсов государства.

Среди известных методов, криптографические методы занимают особое место. При построении механизмов защиты в распределенных информационно-телекоммуникационных системах обычно применяются криптографические преобразования с открытым ключом, к недостаткам которых следует отнести невысокую пропускную способность, громоздкость. Сильное влияние на производительность оказывают арифметические операции в кольцах и полях: умножение, деление, сложение, возведение в квадрат, приведение по модулю и инвертирование. В связи с этим, актуальной научно-технической задачей является повышение производительности современных криптографических преобразований посредством увеличения производительности операций в кольцах и полях целых чисел.

В своих исследованиях авторы сконцентрировались на улучшении производительности операции целочисленного деления, которые основаны на алгоритме Евклида. В работе рассматривается именно расширенный алгоритм Евклида (РАЕ) для

деления больших целых чисел, результатом которого является остаток и частное:

(1) Делимое и делитель – большое целое число одинарной точности.

(2) Делимое – большое целое число двойной точности, а делитель большое целое число одинарной точности, т.е. двоичная длина делимого в 2 раза превышает длину делителя. Эта специфика вытекает с операции умножения двух больших чисел одинарной точности, результатом которой является число двойной точности.

Авторами были изучены известные реализации PAE и сформулированы основные направления его усовершенствования:

• при сравнении больших целых чисел изначально использовать сравнение номеров старших битов, а в случае их равенства, проводить сравнение больших чисел лишь по значимым словам, которые известны благодаря знанию закона изменения параметров уравнения Безу [1];

• при выполнении таких элементарных операций, как вычитание и сдвиг лишь по значимым словам, которые известны благодаря знанию закона изменения параметров уравнения Безу [1].

Сформулированные направления усовершенствования классического PAE нашли место в модифицированном PAE, предложенном авторами.

Была произведена оценка вычислительной сложности классического и модифицированного PAE. Для (1) случая, выигрыш составил 1,46-190,85 раз по количеству операций сравнения и 1,93 – 2,88 раз по арифметическим операциям (начиная с числа 256 бит), с ростом двоичной длины большого целого числа. Во (2) случае выигрыш составил 1,24-196,91 раз по количеству операций сравнений и 1,34-3,26 раз по арифметическим операциям, с ростом двоичной длины большого числа. Арифметические операции быстрее выполняются на современных процессорах и их можно распараллелить, в отличии от операций сравнений. В MPAE операции сравнения сведены до минимума.

Вычислительная сложность MPAE линейно зависит от разности двоичной длины делимого и делителя, что ограничивает область применения PAE/MPAE в случае значительной разницы в двоичных длинах делителя и делимого. В таких случаях следует применять другие алгоритмы.

Для оценки эффективности усовершенствований, были проведены эксперименты на числах, длина которых изменялась в диапазоне от 64 до 16 384 бит. Для усреднения результатов на 1 млн. итераций, для вычислительных систем под управлением процессоров Intel Core i3-M350, Intel Xeon E5 2640 на операционной системе Microsoft Windows 7 x86-64. При 32-битной программной реализации на языке C++ использовался компилятор Microsoft Visual C++ 2010 в режиме оптимизации /O2, с поддержкой расширений SSE2.

С помощью предложенного MPAE, для деления больших целых чисел, удалось повысить производительность программной реализации на указанных вычислительных системах в 1,5-3 раза с ростом двоичной длины целого числа: в случае (1) для чисел длиною от 512 бит и в случае (2) – от 128 бит.

В связи с тем, что MPAE не заложена возможность распараллеливания, не удалось полностью реализовать потенциал современных многоядерных процессоров. Однако, в дальнейшем, планируется воспользоваться арифметикой с отложенным переносом [2], для операций сложения, вычитания и сдвига, что позволит уменьшить внутреннюю связность алгоритма MPAE для эффективного распараллеливания.

Список литературы

1. L.Lhote, B.Vallée: Sharp Estimates for the Main Parameters of the Euclid Algorithm. LATIN 2006: Theoretical Informatics. Lecture Notes in Computer Science Volume 3887, 2006, pp 689-702.

2. Арифметика с отложенным переносом для целых чисел / А. Охрименко // Захист інформації . - 2014. - Т. 16, № 2. - С. 130-138. - Режим доступу: http://nbuv.gov.ua/j-pdf/Zi_2014_16_2_8.pdf.

УДК 004.056

Принципи захисту інформації за допомогою квантової криптографії

Конопліцька-Слободенюк О.К., викладач
Кіровоградський національний технічний університет, м. Кіровоград

Вст уп. Те, що інформація має цінність, люди усвідомили дуже давно. Захист від витоку конфіденційної інформації до неавторизованих осіб є однією з найважливіших проблем сучасного інформаційного суспільства.

Основна частина. В середині 80-х років XX століття виник новий напрям захисту інформації в телекомунікаційних мережах, що отримав назву квантової криптографії, він швидко розвивається в останнє десятиріччя. Проведений аналіз показав, що квантова криптографія вже зайняла гідне місце серед систем, які забезпечують конфіденційну передачу інформації. Від обговорення переваг та недоліків різних протоколів розподілу ключів науковий світ перейшов до пошуку найбільш вдалих структурних і схемотехнічних рішень, що забезпечують збільшення дальності зв'язку, підвищення швидкості формування ключів і зниження впливу дестабілізуючих факторів. Однією з тенденцій розвитку є вдосконалення елементної бази систем квантової криптографії, що передбачає подолання технологічних складнощів виготовлення компонентів. Природним розвитком систем квантової криптографії є їх інтегрування в локальні телекомунікаційні мережі.

Одним з напрямів квантової криптографії є квантовий безпечний прямий зв'язок, де легітимні користувачі обмінюються квантовими частками по квантовому каналу зв'язку і виконують певні операції і вимірювання над цими частками, а також обмінюються додатковою інформацією по звичайному (не квантовому) каналу зв'язку з автентифікацією. Практично в якості квантових часток використовують фотони, а як квантові канали – оптоволоконні лінії зв'язку. При цьому безпека передачі інформації з використанням квантових протоколів безпечного зв'язку гарантується законами квантової фізики. Використовуючи квантові явища, можна спроектувати і створити таку систему зв'язку, яка завжди може виявляти підслуховування. Це забезпечується тим, що спроба виміру взаємозв'язаних параметрів в квантовій системі вносить до неї порушення, руйнуючи вихідні сигнали, а значить, по рівню шуму в каналі легітимні користувачі можуть розпізнати міру активності перехоплювача.

Найпростішим способом знімання інформації у звичайних оптичних телекомунікаційних мережах є розділення пучка фотонів. Однак у протоколах квантової криптографії передавання повинно відбуватися за допомогою одиночних фотонів, і в такому випадку порушник не може відвести частину сигналу. Тому, подібні методи перехоплення інформації не можуть бути застосовані у системах квантової криптографії в ідеальних умовах однофотонних сигналів (до того ж, такі джерела сигналів поки що не створені). На практиці наразі використовують слабкі когерентні імпульси, випромінювані лазерними світлодіодами. Число фотонів в імпульсі визначається розподілом Пуассона, тобто частина переданих імпульсів містить два й більше фотони.

Хоча в теорії квантові системи зв'язку не дозволяють приховано перехоплювати інформацію, практичні реалізації не можна назвати невразливими. По-перше, проблема перешкод і великої відстані не дозволяє передавати поодинокі фотони. Звичайно, їх число зводять до мінімуму, але, раз фотонів більше одного, з'являється теоретична можливість перехопити один фотон і дізнатися його стан, не чіпаючи інші. По-друге, приблизно стокілометровий ліміт відстані для роботи квантових систем різко звужує спектр

використання технології. Навіть, якщо користувачі готові розщедритися на прямий оптоволоконний канал між ними, географічно рознесені точки спілкуватися без «репітера», проміжної точки, не зможуть, а це очевидно вразливе місце для прослуховування і атаки «людина посередині». По-третє, хакери від науки виявили, що «засліплюючи» фотодетектори потужним лазером, можна маніпулювати їх показниками, що дозволяє фальсифікувати дані в системах квантового розподілу ключів. Правда, ці вразливості відносяться до недоліків реалізації, а не концепції, і їх цілком можна здолати в майбутньому.

Невід'ємним атрибутом квантової криптографії є так званий "відкритий" канал зв'язку. Відкритим називається канал, якщо передана по ньому інформація може бути доступна будь-якому учаснику протоколу, в тому числі зловмисникові. Важливою умовою використання відкритого каналу в квантовій криптографії є неможливість змінити передану по ньому інформацію. Таким каналом може виступати, наприклад, Інтернет.

Квантова криптографія дозволяє виявити будь-які спроби прослуховування переговорів і забезпечити секретність переданої інформації за допомогою фундаментальних законів природи, а не технічних чи обчислювальних обмежень зловмисника. Одним з вузьких місць в криптографії досі залишається передача і періодична зміна криптографічних ключів. Йдеться про систему розподілу ключів, призначеної для автоматичного (без участі оператора) генерування та зміни загальних ключів за допомогою передачі однофотонних станів за звичайними (відкритими) оптоволоконними лініями зв'язку.

Будь-який протокол квантового розподілу ключа, яких відомо на сьогоднішній день близько десятка, як невід'ємну частину містить принципову величину - критичний відсоток помилок. Що це означає? Після обміну інформацією у вигляді біт, які записані на фотонах, дві легітимних сторони відкривають частину цієї послідовності і перевіряють кількість помилок. Потім вони, природно, цю частину викидають з цілим ключем із загальної послідовності. Але, перевіривши, яка частина помилок знаходиться у відкритій частині, вони можуть достовірно сказати, просто по ймовірності, чи є той масив даних, який у них залишився, придатним для подальшої обробки, тобто чистки, чи ні. Якщо відсоток помилок перевершує критичний , тоді спілкування вважається несекретним.

Висновки. Зараз одним з найважливіших досягнень в області квантової криптографії є те, що вчені змогли показати можливість передачі даних по квантовому каналу з швидкістю до 1 Мбіт/с. Це стало можливо завдяки технології розділення каналів зв'язку по довжинах хвиль і їх одноразового використання в загальному середовищі. Що до речі, дозволяє одночасне використання як відкритого, так і закритого каналу зв’язку. Експериментальні дані дозволяють зробити прогноз на досягнення кращих параметрів в майбутньому.

Безумовно, квантова криптографія – дуже перспективна частина криптографії, адже технології, використовувані там, дозволяють вивести безпеку інформації на найвищий рівень. Залишилося трохи почекати, і вже дуже скоро квантова криптографія забезпечить ще один шар безпеки для організацій, які в цьому зацікавлені.

Список літератури:

1. Владимир Красавин. Квантовая криптография. Подводная Лодка, №8, 2000.
2. Артамонов В.А. «Квантовая криптография: мифы и реальности» – Журнал «ИТ-Защита» 11 мая 2013
3. Кулик С. Квантовая криптография. – Фотоника. Выпуск #3/2010

УДК 004.056.55

Композиционное универсальное хеширование по кривым Судзуки

Котух Е.В., аспирант кафедры БИТ
Научный руководитель – Халимов Г.З., д-р техн. наук, профессор
Харьковский национальный университет радиоэлектроники, г. Харьков

Безусловная аутентификация реализуется на основе строго (почти строго) универсального хеширования в композиционной конструкции Стинсона [1]. Композиционные схемы являются эффективным механизмом построения класса хеш функций с заданными комбинаторными свойствами. Композиционное включение хеш функций с целью уменьшения размера хеш кода приводит к увеличению вероятности коллизии и увеличению сложности вычислений и, возможно размера ключевых данных.

Предлагается метод каскадного хеширования с универсальным хешированием по кривым Судзуки в первом каскаде и строго универсальным хешированием во втором, как дальнейшее развитие композиционной схемы хеширования.

Для построения строго универсального хеширования применяется метод ортогональных массивов и метод сумм экспонент Вейля-Карлитца-Ушиямы (ВКУ).

Хеширование по рациональным функциям кривых Судзуки в первом каскаде является определяющим для оценки вероятности коллизии. Наилучшие результаты достигаются на максимальных кривых над конечным полем размерности q. Практические вычисления по ортогональным массивам требуют одно вычисление в каскаде строгого универсального хеширования. Вычисления по слабо смещенным массивам $(q^2,2)_q$, $(q^2,4)_q$ увеличивают число вычислений на 2 и 4, и в 2 - 4 раза уменьшают вероятность коллизии в композиционной схеме. Применение строго универсального хеширования позволяет уменьшить размер результирующего хеш кода до энтропийного значения. Реализация строгого (почти строгого) универсального хеширования приводит к трех и четырёхкратному увеличению размера ключевого пространства.

Для фиксированной вероятности коллизии и числа хешируемых слов данных композиционная конструкция с кривыми Судзуки является более эффективной по ключевым затратам по сравнению с хешированием по проективной прямой.

Пусть F_{2^m} определяет хеширование по кривой Эрмита и F_{2^ℓ} - хеширование по проективной кривой. Фиксируем вероятность коллизии

$$\varepsilon = k / 2^\ell = (3k)^{1/3} / 2^m .$$

Получим

$$2^\ell = 2^m k^{2/3} / 3^{1/3} \approx 2^m k^{2/3} .$$

Пусть $k = 2^{m/2}$ и $2^\ell = 2^{m+m/3}$. Рассмотрим строго универсальное хеширование по кривой Сузуки $\varepsilon_1 - SU(2^{4m}, 2^{km}, 2^m)$, $\varepsilon_1 = (3k)^{1/3} / 2^m$ с отображением $f(x) = \phi(ax) + z$, $\phi : F_{2^m} \to F_{2^m}$. Эквивалентное по вероятности коллизии строго универсальное хеширование по проективной прямой $k / 2^\ell - SU(2^{3\ell}, 2^{k\ell}, 2^\ell)$ имеет параметры $k / 2^{m+m/3} - SU(2^{4m}, 2^{k(m+m/3)}, 2^{m+m/3})$. Если $k = 2^m$ и $2^\ell = 2^{m+2m/3}$, тогда

$k / 2^{m+2m/3} - SU(2^{5m}, 2^{k(m+2m/3)}, 2^{m+2m/3})$. Чем больше размер хешируемых данных, тем больше выигрыш по ключевому пространству.

Выводы.

1. Строгое (почти строгое) универсальное хеширование в расширенном поле F_{2^m} допускает отображение $\phi : F_{2^m} \to F_{2^n}$. Имеем оптимизацию затрат на размер ключей $2m+n$ и значение 2^{-n} определяет нижнюю границу значения вероятности коллизии. С помощью отображения $\phi : F_{2^m} \to F_{2^n}$ размер хеш кода приводится к энтропийному значению.

2. Ключевое пространство при переходе от универсального хеширования к строгой (почти строгой) аутентификации в расширенном поле F_{2^m} увеличивается как в случае простого и квадратичного поля.

3. Для фиксированного поля вычислений и числа хешируемых слов данных композиционная конструкция с кривыми Судзуки имеет меньшую вероятность коллизии по сравнению с хешированием по проективной прямой, за счет универсального хеширования первого каскада.

4. Композиционная конструкция по кривой Ферма с большим числом точек имеет оценки вероятности коллизии которые совпадают с строгим хешированием по максимальным кривым в квадратичном поле.

Список литературы

1. Stinson D.R. Universal hashing and authentication codes. / D.R.Stinson // Designs, Codes and Cryptography. – 1994. – N.4. - P.369–380.

УДК 004.056.55

Статистичні дослідження генератора ключових потоків SNOW 2.0

Кузнецов О.О., д-р техн. наук, професор,
Мордвінов Р.І., канд. техн. наук,
Костенко С.В., студент 5 курсу
Харківський національний університет імені В.Н.Каразіна, м. Харків

Криптографічний алгоритм SNOW-2 є словоорієнтованим синхронним потоковим шифром [1 - 3]. За специфікацією цей генератор ключових потоків оперує 32-розрядними словами та застосовується з двома можливими довжинами ключів: 128 і 256 біт. Шифр розроблений відповідно до схеми підсумовуючого генератору ключових потоків та належить до класу схем з рівномірним рухом регістру.

Схема формування ключових потоків складається з лінійного рекурентного регістра довжиною 16 над GF (2^{32}), який задає стан кінцевого автомату (КА). КА складається з блоку підстановки і двох 32-розрядних регістрів. У ньому для формування вихідного ключового потоку і подальшого оновлення стану регістрів використовуються операції додавання по модулю 2^{32} і по модулю 2. Таким чином лінійний рекурентний регістр формує послідовність великого періоду, а кінцевий автомат реалізує спеціальну функцію ускладнення, яка і

забезпечує потрібні криптографічні властивості.

Схематичне подання перетворень відповідно до специфікації генератору ключових потоків SNOW-2 наведено на рис. 1.

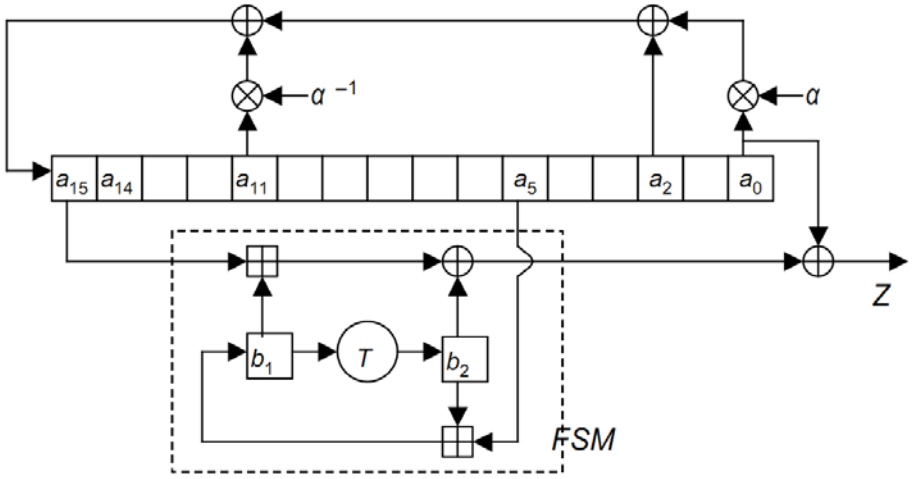

Рисунок 1 – Схематичне подання перетворень генератору SNOW-2

Формування ключових потоків містить наступні процедури:

- функції ініціалізації Init та наступного стану Next, які призначено, відповідно, для формування початкового та наступного значення змінної стану;
- функція ключового потоку Strm, яка формує вихідний ключовий потік;
- функція T, яку заснованою на компонентах із алгоритму блокового симетричного шифрування AES (Advanced Encryption Standard) стандарту [4, 5] та яка виконує підстановку вхідних елементів, зокрема, реалізує перестановку елементів $GF(2^{32})$;
- функції перетворення елементів в кінцевому полі $GF(2^{32})$;
- спеціальна функція ускладнення *FSM (x, y, z)*, яку побудовано із застосуванням різних модульних перетворень (по модулю 2^{32} і по модулю 2).

Генератор ініціюється допомогою двох змінних: секретного ключа k і відомої змінної ініціалізації (IV). Установка ключа здійснюється наступним чином. Секретний вихідний ключ k представляється як $k = (k_1, k_2, k_3, k_4)$ для 128-бітного ключа і $k = (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$ для 256-бітного ключа. При 128-бітному ключі він вводиться в регістр зсуву наступним чином:

$$s_{15} = k_3 \oplus IV_0,\ s_{14} = k_2,\ s_{13} = k_1,\ s_{12} = k_0 \oplus IV_1,$$
$$s_{11} = k_3 \oplus 1,\ s_{10} = k_2 \oplus 1 \oplus IV_2,\ s_9 = k_1 \oplus 1 \oplus IV_3,\ s_8 = k_0 \oplus 1,$$

аналогічно для другої половини,

$$s_7 = k_3,\ s_6 = k_2,\ s_5 = k_1,\ s_4 = k_0,$$
$$s_3 = k_3 \oplus 1,\ s_2 = k_2 \oplus 1,\ s_1 = k_1 \oplus 1,\ s_0 = k_0 \oplus 1,$$

де «1» позначає 32-бітний одиничний вектор.

При 256-бітовому ключі регістр зсуву ініціюється за правилом:

$$s_{15} = k_7 \oplus IV_0,\ s_{14} = k_6,\ s_{13} = k_5,\ s_{12} = k_4 \oplus IV_1,$$
$$s_{11} = k_3,\ s_{10} = k_2 \oplus IV_2,\ s_9 = k_1 \oplus IV_3,\ s_8 = k_0,$$
$$s_7 = k_7 \oplus 1,\ s_6 = k_6 \oplus 1 \ldots,\ s_0 = k_0 \oplus 1.$$

За стандартною схемою передбачається, що $IV_1 = IV_2 = 0$. Після ініціалізації лінійного регістру зсуву значення b_1 і b_2 також встановлюються в нуль. Схема запускається декілька разів, без генерації вихідної послідовності. В результаті на кожному циклі роботи КА формується нове значення регістру. Після певного числа циклів регістр зсуву, а також b_1 і b_2

приймають значення, обчислені на останньому циклі. З цього і починається генерація ключових потоків.

При проведені досліджень було програмно реалізовано алгоритм формування ключових потоків SNOW 2.0 за схемою, що наведено на рис. 1. Проведено статистичні дослідження вихідних послідовностей у різних режимах із застосуванням як 128-ми так і 256-ти бітного ключа. Дослідження проводилися за методикою NIST STS, відповідно до якої виконується 15 незалежних статистичних тестів (з урахуванням різних вхідних параметрів проводиться 188 тестів), по кожному з яких обчислюється відповідна ймовірність проходження тесту. Ця ймовірність використовується правилом прийняття суджень (критерієм згоди) про істинність або хибність гіпотези, щодо певних статистичних властивостей. Аналіз отриманих результатів свідчить, що досліджувані послідовності ключових потоків мають дуже високі показники статистичної безпеки. Для всіх випадків отримані результати з високим проходженням статистичних тестів.

Список літератури

1. Sosemanuk, a fast software-oriented stream cipher. [Електронний ресурс]. Режим доступу: https://www.rocq.inria.fr/secret/Anne.Canteaut/Publications/sosemanuk.pdf

2. Patrik Ekdahl, Thomas Johansson. A New Version of the Stream Cipher SNOW. [Електронний ресурс]. Режим доступу: http://saluc.engr.uconn.edu/refs/stream_cipher/ekdahl02SNOW2.pdf

3. Two versions of the stream cipher snow. A thesis submitted to the graduate school of natural and applied sciences of middle east technical university by Erdem Yilmaz. [Електронний ресурс]. Режим доступу: http://etd.lib.metu.edu.tr/upload/12605592/index.pdf

4. Daemen J. AES proposal: Rijndael/ J. Daemen, V. Rijmen // 1998. [Електронний ресурс]. Режим доступа: http://www.nist.gov/aes.

5. FIPS-197: Advanced Encryption Standard (AES) // National Institute of Standards and Technology. - 2001. – [Електронний ресурс]. Режим доступа: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

УДК 004.056

Огляд алгоритму шифрування «Ель-Гамаля»

Куницька С.Ю., канд. техн. наук, доцент,
Багачук О.П., студент 4 курсу
Черкаський державний технологічний університет, м. Черкаси

В даний час виключно важливе значення в різних наукових областях набули питання, пов'язані зі збереженням і передачею конфіденційної інформації. Виникаючі при цьому завдання вирішує криптографія - наука про методи перетворення інформації в цілях її захисту від незаконних користувачів.

Значення криптографії виходить далеко за рамки забезпечення секретності даних. По мірі все більшої автоматизації передачі та обробки інформації, а також інтенсивності інформаційних потоків її методи набувають унікальне значення.

У 1976 році американські фахівці з обчислювальних наук Уітфрід Діффі (Diffie) і Мартін Хеллман (Hellman) запропонували два нових принципи організації засекреченого зв'язку без попереднього постачання абонентів секретною інформацією (ключами) - принцип так званого "відкритого шифрування" і принцип "відкритого розподілу ключів". Цей момент можна вважати початком нового періоду в розвитку криптографії.

Схема Ель-Гамаля (Elgamal) - криптосистема з відкритим ключем, заснована на труднощах обчислення дискретних логарифмів в кінцевому полі. Криптосистема включає в себе алгоритм шифрування і алгоритм цифрового підпису. Схема Ель-Гамаля лежить в

основі початкових стандартів електронного цифрового підпису в США (DSA) і Росії (ГОСТ Р 34.10-94).

Схема була запропонована Тахером Ель-Гамалем в 1985 році [1], який розробив та удосконалив один з варіантів алгоритму Діффі-Хеллмана. На основі зробленого, було отримано два алгоритми, які використовувалися для шифрування і для забезпечення аутентифікації. На відміну від RSA алгоритм Ель-Гамаля не запатентований і, тому, став більш дешевою альтернативою, оскільки не була потрібна оплата внесків за ліцензію. Вважається, що алгоритм потрапляє під дію патенту Діффі-Хеллмана.

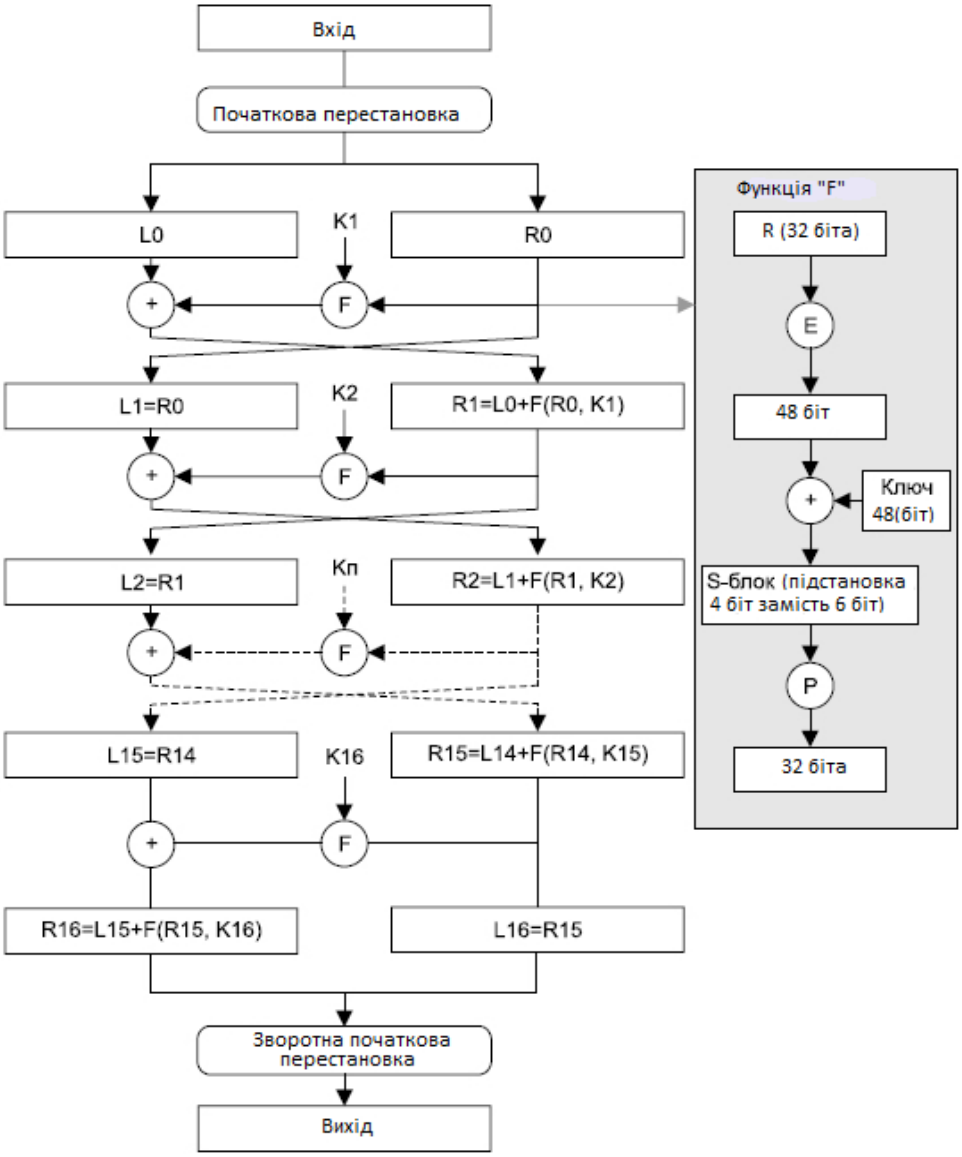

Рисунок 1 – Схема роботи алгоритму шифру Ель-Гамаля

Генерація ключів:

1. Генерується випадкове просте число p.
2. Вибирається випадкове ціле число g таке, що $1 < g < p$.
3. Вибирається випадкове ціле число x таке, що $1 < x < p$.
4. Обчислюється $y = g^x \bmod p$.
5. Відкритим ключем є трійка (p, g, y), закритим ключем - число x.

Шифрування

1. Вибирається сесійний ключ - випадкове ціле число k таке, що $1 < k < p - 1$.
2. Обчислюються числа $a = g^k \bmod p$ і $b = y^k \, k \, M \bmod p$.

3. Пара чисел (a, b) є шифротекстом.

Неважко бачити, що довжина зашифрованого тексту у схемі Ель-Гамаля довша вихідного повідомлення M вдвічі.

Дешифрування

Знаючи закритий ключ x, вихідне повідомлення можна обчислити з зашифрованого тексту (a, b) за формулою:

$$M = b\,(a^x)^{-1} \mod p. \quad (1)$$

При цьому неважко перевірити, що:

$$(a^x)^{-1} \equiv g^{-kx} \pmod p \quad (2)$$

і тому:

$$b\,(a^x)^{-1} \equiv (y^k M)\, g^{-xk} \equiv (g^{xk} M)\, g^{-xk} \equiv M \pmod p. \quad (3)$$

Для практичних обчислень більше підходить наступна формула:

$$M = b\,(a^x)^{-1} \bmod p = b \cdot a^{(p-1-x)} \mod p \quad (4)$$

Криптостійкість та особливості

В даний час криптосистеми з відкритим ключем вважаються найбільш перспективними. До них належить і схема Ель-Гамаля, криптостійкість якої заснована на обчислювальній складності проблеми дискретного логарифмування, де за відомими p, g і y потрібно обчислити x, що задовольняє рівняння:

$$y \equiv g^x \pmod p.$$

Застосування

Алгоритм шифрування Ель-Гамаля використовується для забезпечення підтвердження цілісності та автентичності електронних документів, файлів та інших електронних ресурсів.

Приклад

1. Припустимо, що потрібно підписати повідомлення ~M = baaqab.
2. Зробимо генерацію ключів:
   - нехай p = 23 g = 5 змінні, які відомі деяким персонам.
   - таємний ключ x = 7 - випадкове ціле число x таке, що 1 < x < p.
3. Обчислимо відкритий ключ y: $y = g^x \bmod p = 5^7 \mod 23 = 17$. Отже, відкритим ключем є трійка (p, g, y) = (23,5,17).
4. Тепер обчислимо хеш-функцію: h (M) = h (baaqab) = m = 3.
5. Виберемо випадкове число k таке, що виконується умова 1 < k < p-1. Нехай k = 5.
6. Обчислимо $\sim r = g^k \bmod p = 5^5 \mod 23 = 20$.
7. Обрахуємо число $s \equiv (m - xr)\, k^{-1} \pmod{p-1}$. Таке s існує, так як НОД (k, p-1) = 1. Отримаємо, що s=21.
8. Отже, ми підписали повідомлення: < baaqab, 20,21>.

Список літератури

1. Колеснікова О.О., Пірус Є.М., Рябухо О.М. – Реалізація шифру Ель Гамаля.
2. Онацкий А. В., Йона Л. Г. – Асимметричные методы шифрования. Шифр Ель Гамаля.
3. Ель-Гамаль (алгоритм) – Википедия: http://ru.wikipedia.org/wiki/Схема_Эль-Гамаля_(алгоритм).
4. Мухачев В.А., Хорошко В.А. Методы практической криптографии. – К.: ООО «Полиграф-Консалтинг», 2005. 215 с.
5. Смарт Н. Криптография. – М.: Техносфера, 2005. – 528 с.
6. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 725 с.

УДК 003.26:004.056.55

Аналіз базових груп операцій криптографічного перетворення

Миронюк Т.В., асистент,
Сисоєнко С.В., аспірант,
Миронець І.В., канд. техн. наук, доцент
Черкаський державний технологічний університет, м. Черкаси

За результатами обчислювального експерименту було визначено, що кількість базових груп операцій криптографічного перетворення, які утворюють математичну групу операцій становить 764 базових груп операцій.

Кожна базова група операцій криптографічного перетворення має свій порядковий номер, а елементарні операції для кодування та декодування, що відповідають базовим групам операцій, позначенні кодами функцій [1].

Для подальших досліджень трьохрозрядних операцій криптографічного перетворення представимо основні елементарні функції у наступному вигляді:

$$f_m^{(1)}(x_1, x_2, x_3),$$
$$f_m^{(2)}(x_1, x_2, x_3),$$
$$f_m^{(3)}(x_1, x_2, x_3)$$

– це функції перетворення першого, другого та третього розряду інформації відповідно, що являють собою дискретні логічні функції.

m – це номер елементарної функції в операції криптографічного перетворення.

x_1, x_2, x_3 – значення першого, другого, третього розрядів інформації відповідно.

Відомо, що $x_1, x_2, x_3 \in \{0;1\}$, а відповідно і значення дискретних логічних функцій

$$f_m^{(1)}, f_m^{(2)}, f_m^{(3)} \in \{0;1\}.$$

Так як операції криптографічного перетворення синтезуються на основі вибраних елементарних функцій, то їх можна представити у вигляді композиції відповідних функцій перетворення:

$$F_{1,2,3} = \left(f_m^{(1)}, f_m^{(2)}, f_m^{(3)}\right).$$

Звідси випливає, що елементарні функції $f_m^{(1)}, f_m^{(2)}, f_m^{(3)}$ утворюють операцію криптографічного перетворення.

Дослідивши отримані в наслідок обчислювального експерименту базові групи операцій криптографічного перетворення було визначено, що всі визначені групи базових операцій складаються з 8-ми операцій криптографічного перетворення, а множину елементарних функції, що утворюють операції криптографічного перетворення можливо використовувати як для перетворення, так і для оберненого перетворення відповідно. Надалі будемо називати такі відповідні пари як криптографічна операція перетворення F^k та криптографічна операція оберненого перетворення F^d інформації відповідно.

Представимо, відповідно до визначених позначень, базову групу операцій криптографічного перетворення в явному вигляді.

Для прикладу, розглянемо базову групу операцій криптографічного перетворення представивши операції криптографічного перетворення в наступному вигляді:

1. $F^k_{92,46,27} = (f_{92}^{(1)}, f_{46}^{(2)}, f_{27}^{(3)}) \Rightarrow F^d_{83,116,78} = (f_{83}^{(1)}, f_{116}^{(2)}, f_{78}^{(3)})$

2. $F^{k}_{53,71,27} = (f^{(1)}_{53}, f^{(2)}_{71}, f^{(3)}_{27}) \Rightarrow F^{d}_{83,29,39} = (f^{(1)}_{83}, f^{(2)}_{29}, f^{(3)}_{39})$

3. $F^{k}_{83,29,39} = (f^{(1)}_{83}, f^{(2)}_{29}, f^{(3)}_{39}) \Rightarrow F^{d}_{53,71,27} = (f^{(1)}_{53}, f^{(2)}_{71}, f^{(3)}_{27})$

4. $F^{k}_{58,29,78} = (f^{(1)}_{58}, f^{(2)}_{29}, f^{(3)}_{78}) \Rightarrow F^{d}_{53,46,114} = (f^{(1)}_{53}, f^{(2)}_{46}, f^{(3)}_{114})$

5. $F^{k}_{197,116,39} = (f^{(1)}_{197}, f^{(2)}_{116}, f^{(3)}_{39}) \Rightarrow F^{d}_{197,116,39} = (f^{(1)}_{197}, f^{(2)}_{116}, f^{(3)}_{39})$

6. $F^{k}_{53,46,114} = (f^{(1)}_{53}, f^{(2)}_{46}, f^{(3)}_{114}) \Rightarrow F^{d}_{58,29,78} = (f^{(1)}_{58}, f^{(2)}_{29}, f^{(3)}_{78})$

7. $F^{k}_{163,71,114} = (f^{(1)}_{163}, f^{(2)}_{71}, f^{(3)}_{114}) \Rightarrow F^{d}_{163,71,114} = (f^{(1)}_{163}, f^{(2)}_{71}, f^{(3)}_{114})$

8. $F^{k}_{83,116,78} = (f^{(1)}_{83}, f^{(2)}_{116}, f^{(3)}_{78}) \Rightarrow F^{d}_{92,46,27} = (f^{(1)}_{92}, f^{(2)}_{46}, f^{(3)}_{27})$

Дослідивши обрану базову групу було визначено, що кожна операція з базової групи операцій криптографічного перетворення може використовуватися, як операція перетворення F^k, так і криптографічна операція оберненого перетворення F^d.

Список літератури

1. Криптографическое кодирование: коллективная монография/ под. ред. В.Н. Рудницкого, В. Я. Мильчевича. – Харьков: Изд-во ООО «Щедрая усадьба плюс», 2014. – 240 с.

УДК 004.056.55

Реалізація клієнт-серверного програмного забезпечення для обміну текстовими повідомленнями з шифруванням RSA

Пахомов О.В., студент 5 курсу
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Останнім часом однією з важливих характеристик програмних засобів обміну повідомленнями стала захищеність інформації, що передається за допомогою цих додатків. Тому шифрування даних стало невід'ємною частиною майже кожного додатку, що забезпечує обмін інформацією.

Мета роботи – розробити додаток типу клієнт-сервер, що реалізує передачу зашифрованих повідомлень між користувачами системи.

Для реалізації шифрування повідомлень було обрано алгоритм шифрування з відкритим ключем RSA. Основним недоліком використання RSA є те, що як і всі інші асиметричні алгоритми шифрування, він повільний в роботі, що робить його непридатним для шифрування великих об'ємів даних. Проте при шифруванні невеликих повідомлень, його швидкість достатня, а рівень захищеності інформації значно вищий, ніж при використанні симетричних алгоритмів шифрування.

Розроблювана в даній роботі система використовує наступний алгоритм обміну ключами:

1. Під час запуску, сервер і клієнт генерують пари ключів: публічний і секретний;

2. Отримавши запит на з'єднання, сервер надсилає свій публічний ключ клієнту, який надіслав запит;

3. Клієнт, отримавши публічний ключ сервера, надсилає підтвердження отримання

ключа і свій публічний ключ серверу;

4. Після отримання сервером підтвердження і публічного ключа клієнта, захищений канал зв'язку між сервером і клієнтом вважається встановленим.

На рисунку 1 наведено схему обміну ключами між сервером і одним клієнтом. На схемі використано наступні позначення: K_{OS} – відкритий ключ сервера, K_{SS} – секретний ключ сервера, C_S – повідомлення зашифроване відкритим ключем клієнта, K_{OC} – відкритий ключ клієнта, K_{SC} – секретний ключ клієнта, C_C – повідомлення зашифроване відкритим ключем сервера.

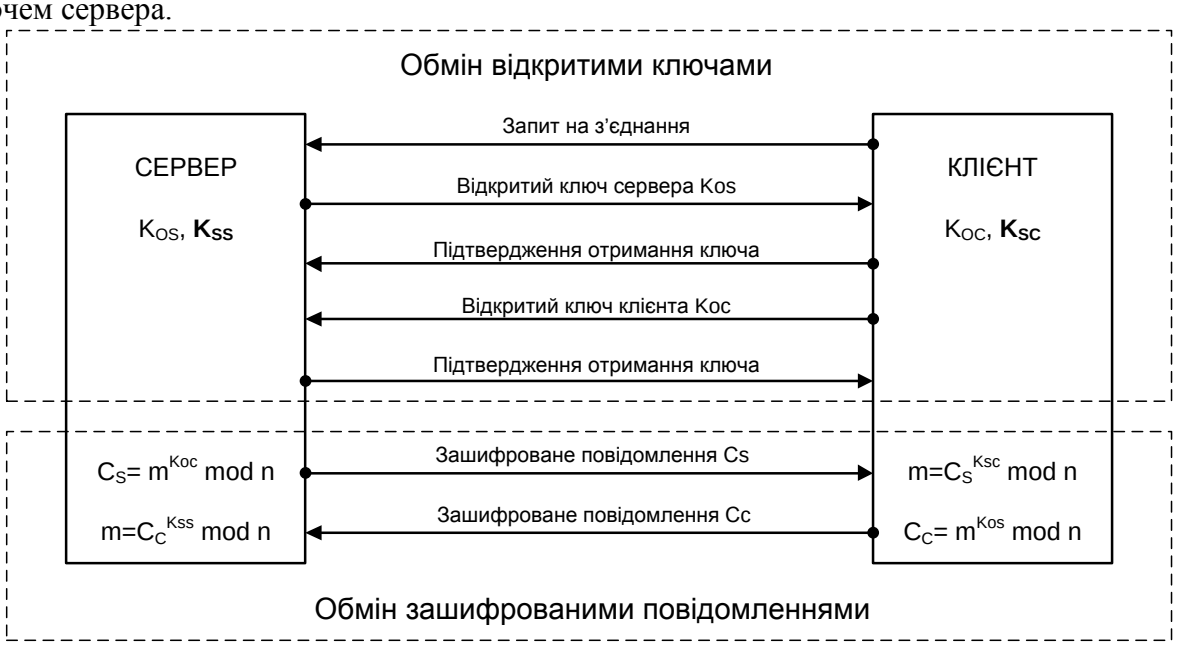

Рисунок 1 – Схема обміну ключами між клієнтом і сервером

Після обміну ключами клієнт шифрує всі повідомлення відкритим ключем сервера і надсилає їх йому. Сервер приймає повідомлення клієнта, дешифрує його своїм секретним ключем, а потім шифрує відповідним відкритим ключем того клієнта, якому адресується повідомлення, і надсилає зашифроване повідомлення клієнту-адресату.

Розглянемо розроблені функціональні схеми системи – функціональну схему серверної (рис. 2) та клієнтської частин (рис. 3) програмного забезпечення системи обміну повідомленнями з шифруванням RSA в комп'ютерній мережі.

Сервер забезпечує передачу зашифрованих повідомлень від одного клієнта іншим. Як видно із схеми, зв'язок з клієнтами здійснюється через локальну мережу, при цьому використовується протокол TCP/IP. На основі IP-адреси сервера та одного з портів (за замовчуванням 8000) створюється прослуховуючий сокет, на який надходять запити на з'єднання від клієнтів. Для кожного підключеного клієнта створюється обслуговуючий сокет та, на основі отриманого від даного клієнта відкритого ключа, RSA-кодер, який виконує шифрування повідомлень для даного клієнта. Також, при запуску сервера, створюється RSA-декодер, який використовує секретний ключ сервера для дешифрування повідомлень, що надходять від клієнтів.

Серверна частина системи включає такі основні функціональні блоки:

- IP-адреса сервера використовується разом з портами для встановлення з'єднання та обслуговування клієнтів;
- RSA-декодер та RSA-кодери кожного клієнта;
- дані сервера: IP-адреса сервера, порт сервера, секретний та публічний ключі сервера, список підключених клієнтів, що містить такі дані про них: IP-адреса, порт підключення, ідентифікатор та публічний ключ клієнта;
- журнал подій, який містить і відображає, на екран або в файл, інформацію про події, що відбуваються в системі.

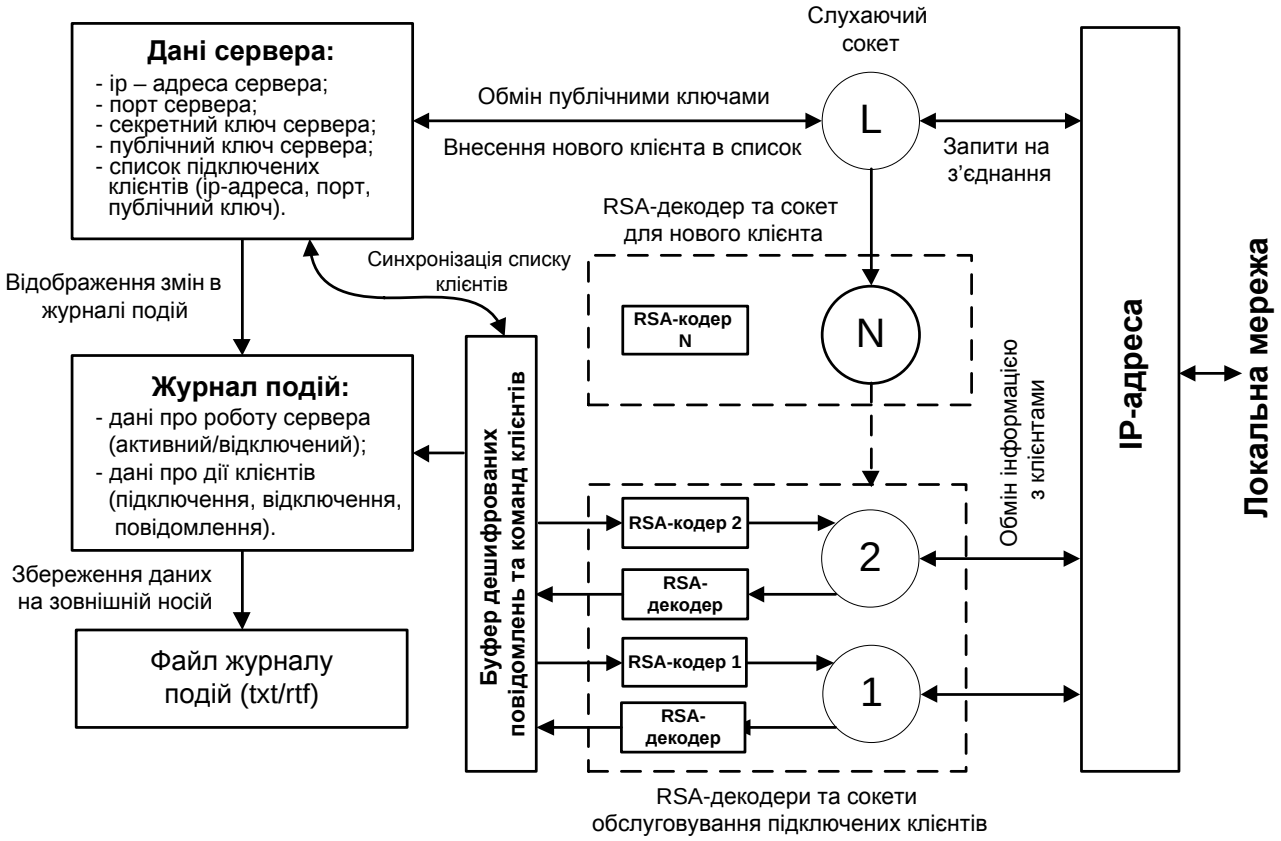

Рисунок 2 – Функціональна схема серверної частини системи

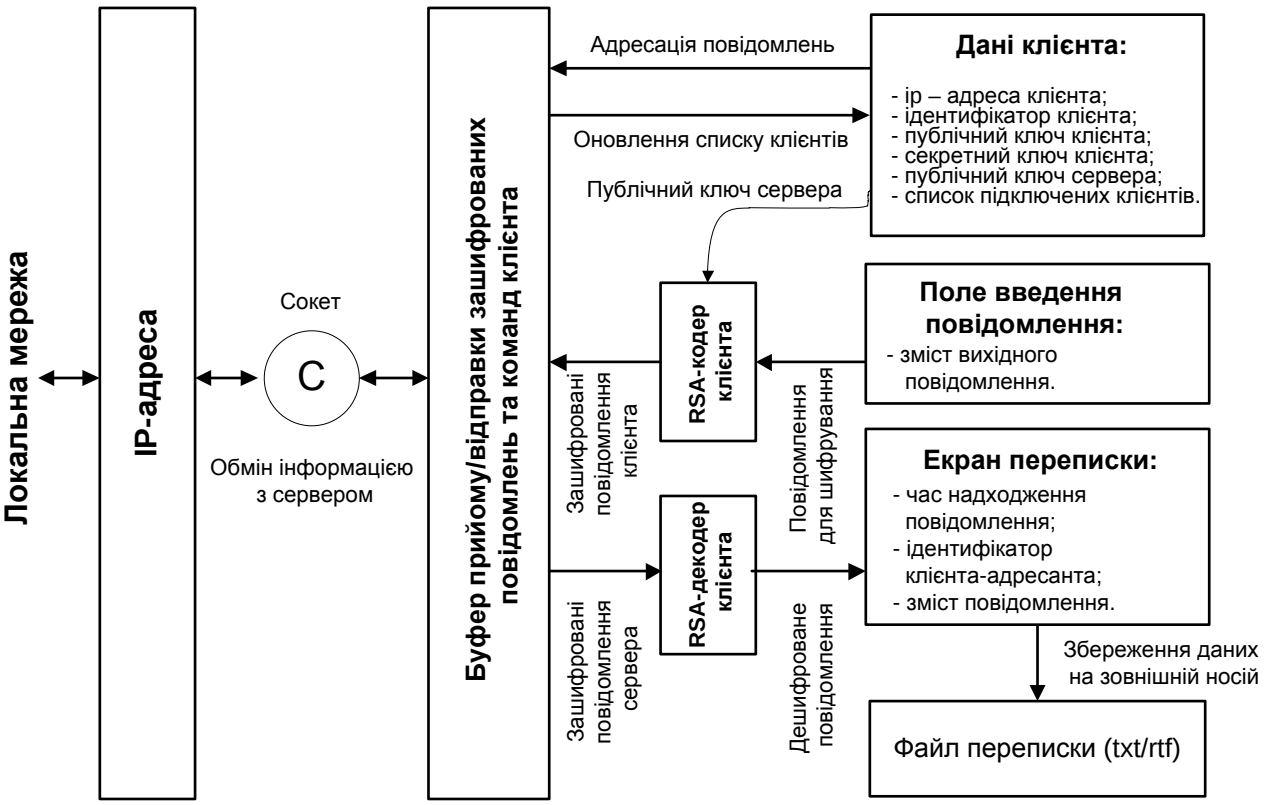

Рисунок 3 – Функціональна схема клієнтської частини системи

На рисунку 3 видно, що клієнт спілкується з сервером через сокет, який створено на основі IP-адреси клієнта та деякого з портів (за замовчуванням 8000). Клієнтська частина програмного забезпечення має один RSA-кодер, що використовує відкритий ключ сервера для шифрування повідомлень, і один RSA-декодер, який дешифрує отримані повідомлення секретним ключем клієнта.

Клієнтська частина системи включає такі основні функціональні блоки:

- IP-адреса клієнта використовується разом з портом для реалізації комунікації з сервером;
- RSA-кодер та RSA-декодер клієнта;
- дані клієнта: IP-адреса клієнта, порт клієнта, секретний та публічний ключі клієнта, список підключених клієнтів;
- поле введення повідомлення;
- екран переписки – функціональний блок, який фіксує та відображає, на екран або в файл, наступну інформацію: час надходження повідомлення, ідентифікатор клієнта-адресанта і зміст повідомлення.

Зв’язок серверної та клієнтської частин системи реалізується через сокети, які являють собою кінцеві точки мережевого з’єднання і забезпечують обмін даними між процесами. В даному випадку процесами, між якими здійснюється обмін даними, є сервер і клієнт, що входять до складу системи.

Розробка програмного забезпечення системи здійснювалася на мові програмування C#, в інтегрованому середовищі розробки Microsoft Visual Studio 2010. Ці засоби програмування являють собою зручний та ефективний інструмент для розробки розподілених додатків, оскільки вони дають можливість використовувати бібліотеки класів .NET Framework, а також ряд технологій та підсистем, що входять до його складу.

Серверна та клієнтська частини прорамного забезпечення реалізовані як додатки з графічним інтерфейсом, для реалізації якого використано інтерфейс програмування додатків Windows Forms, що є частиною платформи Microsoft .NET Framework. На рисунку 4 наведено головне вікно клієнтської частини програмного забезпечення. Воно дає можливість здійснювати обмін зашифрованими повідомленнями з іншими користувачами. На рисунку 5 відображено головне вікно серверної частини системи. Сервер виконує обслуговування клієнтів, які до нього під’єднані.

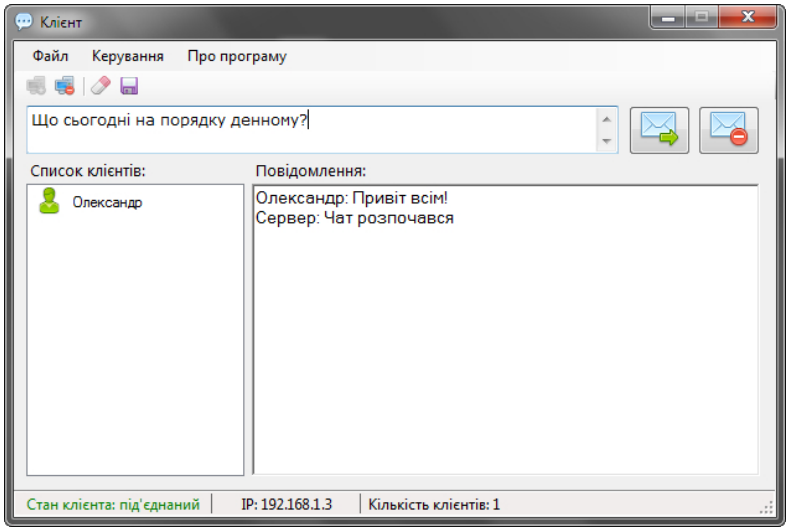

Рисунок 4 – Головне вікно клієнтської частини системи

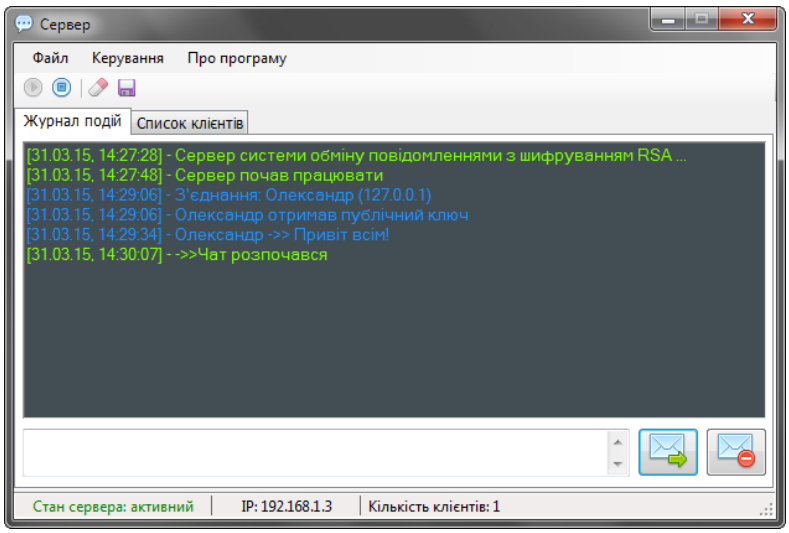

Рисунок 5 – Головне вікно сереверної частини системи

Як серверна, так і клієнтська частини програмного забезпечення мають простий, зручний та типовий, для систем такого типу, інтерфейс користувача. Це забезпечує легкість у освоєнні програмного продукту, зручність у його використанні та відсутність необхідності у здобутті спеціальних знань для його експлуатації.

Розроблене програмне забезпечення дозволяє здійснювати захищений обмін текстовими повідомленнями у локальній мережі або мережі Інтернет та має широку область застосування.

Список літератури

1. Мао В. Современная криптография: теория и практика. : Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 768с.: ил.

2. Двуреченский П.А. RSA – алгоритм шифрования с открытым ключом [Електронний ресурс] // Собрание авторских статей – Режим доступу: http://www.paveldvlip.ru/algorithms/rsa.html.

3. Кровчик Э., Кумар В. NET. Сетевое программирование для профессионалов – М.: «Лори», 2007. – 417с.

4. Дейтел Х. C# в подлиннике: Пер. с англ. / Дейтел Х., Дейтел П., Листфилд Дж., Йегер Ш., Златкина М. – СПб.: БХВ-Петербург, 2006. – 1056 с.:ил.

УДК 004.056.55

Огляд криптографічних технологій захисту інформації

Петровці Ю.І., студентка 4 курсу
Науковий керівник – Кучмеровська Т.М., д-р біол. наук
Національний університет харчових технологій, м. Київ

З розвитком і розширенням сфери застосування обчислювальної техніки, розвитком локальних мереж і підключенням до глобальної мережі постала проблема захисту інформації, яка використовується в цих системах. Інформація, що проникає у всі сфери діяльності суспільства, набуває конкретного політичного, матеріального і вартісного вираження [1]. Тому захист інформації як складна, наукомістка і багатогранна проблема в умовах упровадження сучасних інформаційних технологій, створення розподілених

обчислювальних систем і мереж зв'язку набуває особливої гостроти. Одним із методів захисту інформації являється криптографія.

На сьогодні криптографія, як галузь знань, та криптографічний захист інформації, як окрема галузь діяльності, стосується: питань шифрувальної справи, новітніх технологій електронної торгівлі, систем автоматизованого управління, звітування та контролю [2]. Криптографія (від грецького kryptós - прихований і gráphein - писати) - наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації. Дана наука розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри та теорії ймовірностей. Механізм шифрування може забезпечувати конфіденційність переданих даних або інформації про параметри трафіка. Він може бути використаний у деяких інших механізмах безпеки або доповнювати їх. Існування механізму шифрування припускає використання, як правило, механізму керування ключами [3].

Методи криптографічного захисту інформації – це системи шифрування інформації, алгоритми захисту від нав‘язування фальшивої інформації (MAC-коди та алгоритми електронного цифрового підпису) та криптографічні протоколи розподілу ключів, автентифікації та підтвердження факту прийому (передачі) інформації [4].

Криптографічна стійкість вимірюється тим, скільки знадобиться часу і ресурсів, щоб із шифртексту відновити вихідний відкритий текст. Ніким ще не доведено, що доступне сьогодні стійке шифрування, яке однак не є абсолютно стійким як шифр Вернама (схема одноразових блокнотів, використовувана розвідувальними службами провідних держав світу), зможе встояти проти обчислювальних можливостей комп'ютерів, доступних завтра. Результатом стійкої криптографії є шифртекст, який винятково складно зламати без володіння визначеними інструментами дешифрування. Проте, стійка криптографія, задіяна в PGP, – найкраща стійка криптографія на сьогоднішній день [5].

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. На сьогодні відомо більше десятка перевірених методів шифрування, які при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу (наука "зламування" криптографічних перетворень).

Основні методи криптографічного захисту інформації можуть бути класифіковані різним чином, але найчастіше їх розподіляють в залежності від способу використання та за типом ключа [6]: безключеві – не використовуються ключі (хеш-функції, генерація псевдовипадкових чисел, односторонні перестановки); перетворення з таємним ключем – використовується ключовий параметр – секретний ключ (симетричне шифрування, цифровий підпис, хеш-функції, ідентифікація); перетворення з відкритим ключем – використовують в своїх обчисленнях два ключі – відкритий (публічний) та закритий (приватний) (асиметричне шифрування, цифровий підпис). Цілісність інформації та автентичність сторін досягається використанням хеш-функції та технології цифрового підпису. Конфіденційність інформації забезпечується симетричним та асиметричним методами шифрування.

Отже, у сучасних реальних криптосистемах шифрування даних здійснюється за допомогою «швидких» симетричних блокових алгоритмів, а завданням «повільних» асиметричних алгоритмів стає шифрування сеансового ключа. В цьому випадку зберігаються переваги високої секретності (асиметричні) та швидкості роботи (симетричні).

Список літератури

1. Задірака В.К. Олексик О. Комп‘ютерна криптологія / В. К. Задірака, О. Олексик. – Київ, 2002. – 505 с.
2. Бабаш А.В., Шангин Г.П. Криптография. Под редакцией В.П. Шестюка, Э.А. Применко / А.В. Бабаш, Г.П. Шанкин. – М.:СОЛОН-ПРЕСС, 2007. – 512 с.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с.

4. Бабак В.П. Теоретичні основи захисту інформації / В. П. Бабак: Підручник. – Книжкове видавництво НАУ, 2008. – 752 с.
5. Криптографія [Електронний ресурс]. — Режим доступу: http://uk. wikipedia.org/wiki/Криптографія.
6. Алферов А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Учебное пособие, 2-е изд., испр. и доп. – М.. Гелиос АРВ, 2002. – 480 с.

УДК 004.056.55

Уменьшенная модель шифра ГОСТ 28147-89

Самойлова А.В., аспирант кафедры БИТ
Научный руководитель – Кузнецов А.А., д-р техн. наук, профессор
Харьковский национальный университет радиоэлектроники, Харьков

Анализ криптографических свойств блочных шифров возможен на моделях с малым числом состояний. Этого можно достичь путём ограничения множества ключей или исследуемых входных текстов. Другой подход заключается в исследовании мини версий блочных шифров. Если мини версия адекватно описывает полную версию шифра, можно получить исчерпывающие криптографические свойства шифра по всем ключам и текстам. В этом контексте построение моделей мини версий является актуальным.

В данной работе рассматривается модель мини-версии стандарта симметричного шифрования ГОСТ 28147-89 [1]. Рассматриваемая модель предполагает наличие входных данных, основных преобразований, выходных данных как и у стандартной модели, однако уменьшенных, а также уменьшенное количество циклов шифрования.

Программная реализация была разработана для таких исходных параметров:

1) 8 бит входного текста;
2) 8 бит зашифрованного текста;
3) 16 бит ключевая информация;
4) Количество циклов криптографического преобразования – 16 циклов.

Процесс зашифрования входных данных происходит по схеме, аналогичной стандарту, схематически предлагаемый алгоритм криптопреобразования показан на рис. 1.

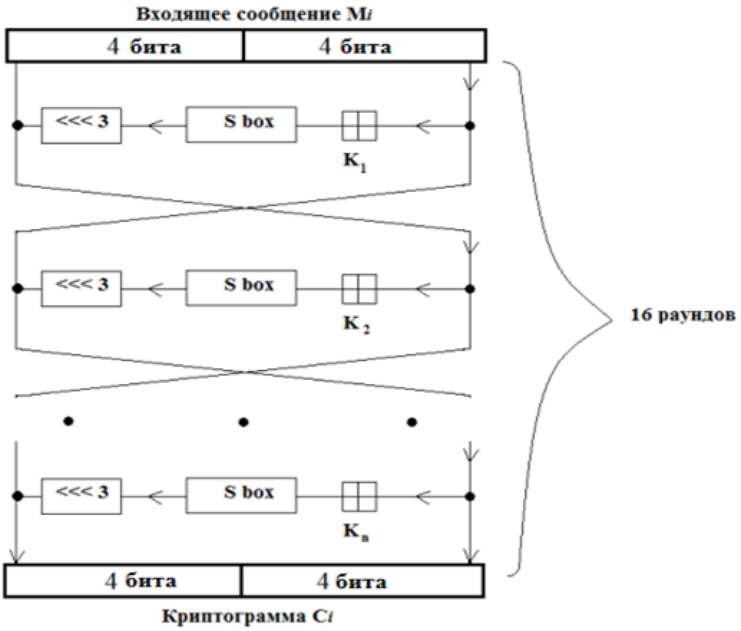

Рисунок 1 — Схема алгоритма зашифрования шифра мини ГОСТ28147-89

Алгоритм ГОСТ есть Фейстель-подобным, преобразования происходят с одним блоком входных данных, который добавляется к другому блоку, и затем блоки меняются местами. На последнем раунде зашифрования блоки не меняются местами.

Алгоритм зашифрования мини версии состоит из следующих операций:

1) входной блок информации разбивается на два подблока по 4 бита каждая;

2) затем выполняется сложение по модулю 2^4 правого подблока с циклическим ключом. Циклический ключ генерируется путем нарезания основной ключевой информации (16 бит) по 4 бита. Полученные ключи подаются в схему шифрования в следующем порядке:

K1, K2, K3, K4, K1, K2, K3, K4, K1, K2, K3, K4, K4, K3, K2, K1;

3) полученный промежуточный результат проходит через один S-box табл. 1;

4) затем происходит циклический сдвиг полученного результата влево на 3 бита;

5) сложение полученного с предыдущего шага результата с левым блоком входного текста по модулю два;

6) обмен данными между левой и правой частью блока.

Таблица 1

S-box

$x_{вх}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$x_{вых}$	4	A	9	2	D	8	0	E	6	B	1	C	7	F	5	3

В процессе зашифрования шаги 2-6 выполняются 15 раз с использованием на каждом раунде 4 битового циклового ключа. В конце 16 раунда подблоки не меняются местами.

Для исследования криптографических свойств данной модели шифра проводилось зашифрование всех возможных сообщений на всех возможных ключах. В результате получили определенный массив криптограмм. Целью исследования было определить количество ключей, при которых C_i=M_i. Также с применением математического аппарата теории вероятностей и математической статистики определялись значения среднего значения, дисперсии, среднего-квадратического отклонения для каждого столбца полученного массива. В таблице 1 приведена часть полученного массива.

Таблица 1

Массив полученных результатов

		Входное сообщение M_i															
		00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
Криптограмма C_i	00	768	512	256	512	0	0	256	256	256	0	256	256	768	0	0	256
	01	256	512	0	512	256	0	512	256	0	512	256	256	256	0	256	0
	02	512	0	512	0	512	256	512	256	256	0	512	256	768	0	0	768
	03	512	0	0	512	256	256	512	768	512	512	0	256	0	256	0	256
	04	256	0	256	512	0	256	512	256	256	0	0	512	256	256	256	256
	05	256	0	0	512	0	0	0	256	0	0	512	256	256	256	0	0
	06	512	0	768	512	256	0	768	256	0	0	0	256	512	768	256	768
	07	0	0	256	256	1024	0	512	256	512	512	256	256	256	512	0	512
	08	0	0	512	768	0	512	256	0	0	0	0	0	256	768	256	512
	09	256	0	256	512	1024	768	256	512	768	256	0	256	256	0	256	256
	0a	0	256	256	256	512	256	256	512	0	256	0	0	256	256	512	256
	0b	0	0	0	256	0	256	0	256	256	0	512	512	512	256	512	256
	0c	256	0	0	256	0	256	512	0	256	0	256	512	0	0	256	256
	0d	0	0	0	0	0	0	256	0	512	256	768	0	256	256	256	512
	0e	0	256	512	512	0	0	768	0	256	0	256	256	512	0	0	256
	0f	512	0	0	256	512	256	0	256	512	0	256	0	512	0	512	768

Значения входных сообщений и полученных криптограмм записаны в шестнадцатеричном виде. Значение ячейки таблицы, это число ключей при которых $C_i=M_i$.

Выводы.

1. В представленной мини версии число внутренних состояний шифра равняется $2^{16}\times2^8$, что позволяет реализовать анализ криптографических свойств блочного шифра за время ~2 часа вычислений на современном компьютере.

2. Адекватность мини версии проверена на тестовых векторах, операции зашифрования и расшифрования выполняются корректно.

3. Задачей, требующей решения является исследование периодических свойств гаммы мини версии, которая генерируется в режиме гаммирования.

Список литературы

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Изд-во стандартов, 1989. – 20 с.

2. Кузнецов, О.О. Періодичні властивості шифргами у режимі OUTPUT FEEDBACK / О.О. Кузнецов, Ю.І. Горбенко, Є.П. Колованова // Прикладна радіоелектроніка. – Х.: ХНУРЕ. – 2014. – Том 13, №2. – с. 239-251.

УДК 004.056.55

Реалізація служби провайдера шифрування на платформі Java

Смірнова Н.В., канд. техн. наук, доцент,
Смірнов В.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Платформа Java визначає ряд API, що охоплюють головні галузі безпеки, включаючи криптографію, інфраструктуру керування відкритими ключами, аутентифікацію, безпечну передачу, і керування доступом. Ці API дозволяють розробникам легко інтегрувати безпеку в свій код програми. Вони були розроблені навколо таких принципів:

- Незалежність реалізації.
- Функціональна сумісність реалізації.
- Розширюваність алгоритму.

Провайдер криптографічних служб (провайдер) звертається до пакету (або ряду пакетів), які надають конкретну реалізацію підмножини аспектів криптографії API безпеки JDK.

У платформі Java клас `java.security.Provider` інкапсулює поняття постачальника систем забезпечення безпеки. Він визначає ім'я провайдера і перелічує служби безпеки, які реалізує. Багаторазові провайдери можуть бути налаштовані одночасно і перелічуються в порядку переваги.

Криптографічна служба завжди зв'язується з певним алгоритмом або типом. Вона забезпечує криптографічні операції:

- для цифрових підписів або оглядів повідомлення, шифрів або протоколів узгодження ключів;
- генерує або надає криптографічний матеріал (ключі або параметри) необхідний для криптографічних операцій;
- генерує об'єкти даних (`keystores` або сертифікати), які інкапсулюють криптографічні

ключі безпечним способом.

Механізм реалізації забезпечує інтерфейс для функціональності певного типу криптографічної служби (незалежний від певного криптографічного алгоритму). Він визначає Прикладний програмний інтерфейс (API), методи якого дозволяють додаткам отримувати доступ до певного типу криптографічної служби, яку він забезпечує.

Наприклад, механізм реалізації класу `Signature` забезпечує доступ до функціональності алгоритму цифрового підпису. Фактична реалізація алгоритму підпису, такого як SHA1 з DSA, SHA1 з RSA, або MD5 з RSA надана в класі `SignatureSPI.`

Інтерфейси додатка, надані механізмом `class`, реалізуються з точки зору Інтерфейсу Постачальника послуг (Service Provider Interface - SPI). Таким чином, для кожного механізму `class` є відповідний абстрактний SPI class, який визначає методи, які повинні реалізувати провайдери криптографічних служб.

Екземпляр механізму `class`, як об'єкт API, інкапсулює екземпляр відповідного SPI, об'єкта SPI.

Всі методи API об'єкта API оголошуються `"final"`, а їх реалізацію викликають відповідні методи інкапсулюючого об'єкта SPI.

Кожний клас SPI абстрактний. Щоб надати реалізацію певного типу служби для певного алгоритму, провайдер повинен розділити відповідний SPI на підкласи типу `class` і забезпечити реалізації для всіх абстрактних методів.

Інстанціруя реалізації провайдера, такі, як `Cipher, KeyAgreement, KeyGenerator, MAC` або `SecretKey` фабрики, платформа визначить кодову базу провайдера (файл JAR) і перевірить його підпис. Таким чином Java Cryptography Architecture (JCA) аутентифікує провайдера і гарантує, що тільки провайдери, підписані об'єктом, які довіряється, можуть бути включені в JCA.

Крім того, кожен провайдер повинен виконати перевірку самоцілісності, для гарантії, що файлом *.JAR не керують ззовні, у спробі викликати методи провайдера безпосередньо, а не через JCA.

Для виключення можливості управління ззовні в обхід JCA, провайдер повинен реалізувати наступне:

Всі класи реалізації SPI у пакеті провайдера повинні бути оголошені `final` (так, щоб вони не могли бути розділені на підкласи), а їх (SPI) методи повинні бути оголошені `protected`.

У всіх crypto-зв'язаних класів у пакеті провайдера повинен бути реалізований приватний контекст пакета, таким чином, щоб до нього не можна було отримати доступ поза пакетом провайдера.

Для провайдерів, які можуть бути експортовані, `CipherSpi` реалізації повинні включати реалізацію методу `engineGetKeySize`, який повертає розмір ключа.

Висновки

Таким чином, реалізація служби провайдера шифрування платформи Java дозволяє легко створювати захищені додатки для роботи з даними, використовуючи механізм цифрового підпису та інші механізми, що підключаються користувачем API і програмного інтерфейсу Service Provider Interface.

Список літератури

1. http://docs.oracle.com/javase/6/docs/api/

2. Robert Seacord Replaceable Components and the Service Provider Interface. Technical Note CMU/SEI-2002-TN-009. The Software Engineering Institute is a federally funded research and development center / Robert Seacord. - U.S. Department of Defense, 2002. - 48 с.

УДК 004.056.55

Универсальное хеширование в простом поле по алгебраическим кривым Гурвица

Халимов О.Г., соискатель по кафедре БИТ
Научный руководитель – Семенов С.Г., д-р техн. наук, профессор
Харківський національний університет радіоелектроніки, м. Харків

Проблематикой универсального хеширования по алгебраическим кривым C над конечным полем F_q является построение алгоритмов вычисления хеш кодов и оценка параметров хеш функций. Наилучший результат достигается на максимальных кривых и кривых с большим отношением числа точек к роду кривой. С этой целью рассмотрено универсальное хеширование по кривой Гурвица в простом поле и практический алгоритм хеширования.

В простом поле не существует максимальных кривых. Наилучший результат по числу точек в простом поле F_q достигается на кривой Гурвица

$$X^{2(q-1)/3}Y^{(q-1)/3} + Y^{2(q-1)/3}Z^{(q-1)/3} + X^{(q-1)/3}Z^{2(q-1)/3} = 0.$$

Кривая имеет $N = 2\left(q-1\right)^2/3$ F_q рациональных точек вида $P_{a,b} = (a:b:1)$, $a,b \in F_q$, $a \neq 0$, $b \neq 0$ $a^{2(q-1)/3}b^{(q-1)/3} + b^{2(q-1)/3} + a^{(q-1)/3} = 0$ и три точки $P_0 = (1:0:0)$, $P_1 = (0:1:0)$, $P_2 = (0:1:1)$. Род кривой $g = \left(q^2 - 5q + 10\right)/6$, при больших значениях q $N/g \approx 4$.

При большом роде проигрыш границе Хассе-Вейля в простом поле для кривых Гурвица пропорционален $1/\sqrt{q}$. С уменьшением рода кривой значение числа точек приближается к границе Хассе-Вейля.

Функциональное поле кривой можно определить рациональными функциями $x = X/Z$, $y = Y/Z$. Базис пространства $L(mP_\infty)$ задается полиномами $x^i \cdot y^j$ [1].

Хеш функция $h_{x,y}(m) \in F_q$ для сообщения m по рациональным функциям базисного пространства $L(\rho_k P_\infty)$ в точке x, y кривой Гурвица определяется выражением

$$h_{x,y}(m) = \sum m_{i,j} \cdot x^i \cdot y^j,$$

где $m_{i,j}$ - слова сообщения.

Замечание.

1. Для хеширования по кривой Гурвица $X^{2(q-1)/3}Y^{(q-1)/3} + Y^{2(q-1)/3}Z^{(q-1)/3} + X^{(q-1)/3}Z^{2(q-1)/3}$ следует в выражении выполнить соответствующую индексацию степеней i и j.

2. Вычисление хеш функции $h_{x,y}(m) \in F_q$ является справедливым для произвольной алгебраической кривой, если функциональное поле кривой определяется рациональными функциями $x = X/Z$, $y = Y/Z$. Вычисления по кривым Эрмита и максимальным кривым второго рода являются подтверждением.

3. Хеширование по алгебраическим кривым на функциональном пространстве $L(\rho_k P_\infty)$ над простым полем F_q определяет универсальный хеш класс $\varepsilon - U(N, q^k, q)$, где N - число точек алгебраической кривой (объём ключевого пространства), q^k - объём пространства сообщений, q - объём пространства хеш кодов. Вероятность коллизии ε определяется соотношением $\varepsilon = \rho_k / N$.

Пример. Пусть задано F_{19} и кривая Гурвица $x^{12}y^6 + y^{12} + x^6 = 0$. Число точек кривой равно $N = 219$. Первые 48 точек кривой представлены в табл. 1. Точки $P_0 = (1:0:0)$ и $P_1 = (0:1:0)$ определяются как точки на бесконечности.

Таблица 1

Точки кривой $x^{12}y^6 + y^{12} + x^6 = 0$

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}
z	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1
y	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	α^1
x	1	0	0	α^1	α^2	α^4	α^5	α^7	α^8	α^{10}	α^{11}	α^{13}	α^{14}	α^{16}	α^{17}	1
	P_{16}	P_{17}	P_{18}	P_{19}	P_{20}	P_{21}	P_{22}	P_{23}	P_{24}	P_{25}	P_{26}	P_{27}	P_{28}	P_{29}	P_{30}	P_{31}
z	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1
y	α^1	α^1	α^1	α^1	α^1	α^1	α^1	α^1	α^1	α^1	α^1	α^2	α^2	α^2	α^2	α^2
x	α^1	α^3	α^4	α^6	α^7	α^9	α^{10}	α^{12}	α^{13}	α^{15}	α^{16}	1	α^1	α^2	α^3	α^5
	P_{32}	P_{33}	P_{34}	P_{35}	P_{36}	P_{37}	P_{38}	P_{39}	P_{40}	P_{41}	P_{42}	P_{43}	P_{44}	P_{45}	P_{46}	P_{47}
z	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1
y	α^2	α^2	α^2	α^2	α^2	α^2	α^2	α^3	α^3	α^3	α^3	α^3	α^3	α^3	α^3	α^3
x	α^6	α^8	α^9	α^{11}	α^{12}	α^{14}	α^{17}	α^1	α^2	α^3	α^4	α^7	α^8	α^{10}	α^{11}	α^{13}

Распределения кратностей пересечения полиномов базисного пространства $L(mP_\infty)$ и кривой Гурвица без точек P_0 и P_1 представлены в табл. 2.

Таблица 2

Распределение кратности пересечения полиномов базисного пространства и кривой $x^{12}y^6 + y^{12} + x^6 = 0$

Базисное пространство	Число испытаний	Распределение кратности пресечения (значение числа точек пересечения = число опытов)			
1,x,y	10^5	12:=9870 14:=89820			
1,x,y,x^2,xy,y^2	10^6	12:=132 13:=1795 14:=36585 15:=151266 16:=208744	17:=88835 18:=52128 19:=35241 20:=63248 21:=45492	22:=90866 23:=49773 24:=65385 25:=48997 26:=17345	27:=36131 28:=8036
1,x,y,x^2,xy,y^2,x^3,x^2y,xy^2,y^3	10^6	13:=51 14:=4050 15:=48141 16:=162630 17:=24716	20:=78734 21:=36718 22:=17148 23:=9543 24:=6683 25:=4796	27:=2055 28:=1088 29:=429 30:=213 31:=75 32:=71	34:=53 35:=53 36:=47 37:=30 38:=18 39:=13

		1 18:=227222 19:=149512	26:=3385	33:=73	40:=7 41:=1
$1,x,y,x^2,xy,y^2,x^3,x^2y,xy^2,y^3,$ x^4,x^3y,x^2y^2,xy^3,y^4	10^6	13:=35 14:=4347 15:=47581 16:=148469 17:=223188 18:=216293	19:=158898 20:=98028 21:=53754 22:=27179 23:=12539 24:=5548	25:=2326 26:=1002 27:=449 28:=184 29:=95 30:=43	31:=18 32:=12 33:=7 34:=3 35:=1 36:=1

Хеш вычисления в конечном поле F_{19} для 10 слов данных по полиномиальному базису $L(42P_\infty)$ на кривой $x^{12}y^6 + y^{12} + x^6 = 0$ дают оценку вероятности коллизии $\varepsilon = m / N = 42 / 217 = 0.193$. Действительно число точек кривой $N = 217$ и число совпадающих хешей при вычислении по полиномиальному базису $L(42P_\infty)$ не превышает значения 42. Это лучше чем по кривой $x^6 + y^6 + z^6$.

Выводы. Лучший результат для хеширования в простом поле дают кривые Гурвица. Требуют решения задачи вычисления порядков полюсов рациональных функций функционального поля кривой и вычисления точек кривой.

Список литературы

1. Халимов Г.З. Оценки универсального хеширования по алгебраическим кривым / Г.З.Халимов, Ю.И.Горбенко // VI Международная научно-практическая конференция «Наука и социальные проблемы общества: информатизация и информационные технологии»: Сборник. научных трудов.- Харьков: ХНУРЭ. - 2011.- С.276-277.

УДК 004.056.55

Открытая ключевая криптография на групповой алгебре

Цапко Д.П., соискатель по кафедре БИТ
Научный руководитель – Халимов Г.З., д-р техн. наук, профессор
Харківський національний університет радіоелектроніки, м. Харків

Криптография с открытым ключом строится на трудности решения математических проблем, которые очень часто, но не исключительно, возникают из теории чисел. В начале 80-х годов, было предложено применение групповых теоретических проблем для криптографии (Wagner и Magyarik [1], Wagner [2], Magliveras [3]). В частности в работах Magliveras и др., были сделаны предложения для криптографических схем, на основе специальных разложений конечных групп (так называемые логарифмические сигнатуры) [Magliveras 86, Magliveras и др. 02]. Кроме того, известны другие криптографические исследования Gonzarlez Vasco, Steinwandt, Birget, Bohliet и др. Эти разложения, как математические объекты интересные сами по себе. Например, работа Hajors о гипотезе

Минковского показывает, что для абелевых групп, этот вид разложения возникает при изучении многомерных покрытий (см. [4]).

Для абелевых групп логарифмическая подпись имеет следующее определение. Пусть H циклическая группа порядка $ord(H)=p^m$ для некоторого простого числа p, и пусть a некоторый генератор H. Тогда $\alpha=[\alpha_1,...,\alpha_m]$ с $\alpha_i=[e_H, a^{p^{i-1}},...,a^{(p-1)p^{i-1}}]$ $(i=1,...,m)$ является логарифмической подписью для H длины $mp=B(H)$. Теперь просто заметить, что сопоставление минимальной длины логарифмической подписей для циклической p-главных факторов абелевой группы G дает минимальную длину логарифмической подписи для G.

Примерами криптосистем с открытым ключом являются MST1, MST2, MST3. Актуальной задачей их реализации является построение коротких логарифмических сигнатур. Логарифмические подписи, особый тип групповых разложений, представляется в качестве основных компонентов некоторых криптографических ключей. Научный интерес связывается с поиском логарифмических подписей минимальной длины в конечных группах. В частности, такие разложения существуют для разрешимых, симметрических и знакопеременных групп.

Анализируются условия существования логарифмических подписей минимальной длины для нескольких семейств конечных групп: проективной специальной группы PSL2(q), группы Янко порядка <175560, группы Судзуки и группы Матье.

Не существует малочисленной группы, для группы Янко - это порядок <175560, для которой можно построить логарифмическую подпись минимальной длины.

Направлением дальнейших исследований является факторизация больших групп и построение автоморфизмов её вложенных подгрупп на числовые поля.

Список литературы

1. N. R. Wagner and M. R. Magyarik. “A Public Key Cryptosystem Based on the Word Problem.” In Advances in Cryptology. Proceedings of CRYPTO 1984, pp. 19—36, edited by G. R. Blakley and D. Chaum, Lecture Notes in Computer Science 196. Berlin: Springer, 1985.

2. N. R. Wagner. “Searching for Public-Key Cryptosystems.” In Proceedings of the 1984 Symposium on Security and Privacy (SSP ’84), pp. 91—98. Los Alamitos, CA: IEEE Computer Society Press, 1990.

3. S. S. Magliveras. “A Cryptosystem from Logarithmic Signatures of Finite Groups.” In Proceedings of the 29th Midwest Symposium on Circuits and Systems, pp. 972—975. Amsterdam: Elsevier Publishing Company, 1986.

4. S. K. Stein and S. Szabor. Algebra and Tiling. Homomorphisms in the Service of Geometry.The Carus Mathematical Monographs, No. 25. Washington, DC: The Mathematical Association of America, 1994.

УДК 004.056.55

Модель атаки із використанням спеціально підібраних повідомлень на цифровий підпис в фактор кільцях поліномів

Шевцов О.В., аспірант денної форми навчання
Науковий керівник – Кузнецов О.О., д-р техн. наук, професор
Харківський національний університет радіоелектроніки, м. Харків

Одним з перспективних напрямків розвитку сучасної криптографії є криптосистема NTRU. Подальший розвиток цієї теми потребує особливої уваги при вивченні захищеності електронного цифрового підпису NTRUSign. В алгоритмі NTRUSign базові операції відбуваються в фактор - кільці поліномів (далі ФКП) $R = Z[X]/(X^N - 1)$. Підпис NTRUSign [1] обчислюється за формулою :

$$s \equiv f * B + F * b(mod\ q); t \equiv g * B + G * b(mod\ q), \quad (1)$$

де B та b обчилюють із співвідношень:

$$G * m_1 - F * m_2 = A + q * B; g * m_1 - f * m_2 = a + q * b). \quad (2)$$

Поліноми a, A мають коефіцієнти із діапазона [-1/2 ,1/2] та $b, B \in Z[X]/(X^N - 1)$. Насамперед $(s,\ t)$ - це підпис, а (f, g, F, G) секретний ключ. Можна обрахувати t інакше: $t = s * h\ (mod\ q)$, для цього знадобиться відкритий ключ h.

Поліном h знаходиться, як $h = f^{-1} * g(mod\ q)$. В свою чергу q обирають, як степінь двійки, а N це розмірність кільця R. При перевірці підпису - обчислюється відстань між векторами $(s,\ t)$ та $(m_1,\ m_2)$, як норма різниці між цими векторами. Ця відстань повинна бути не більше ніж заздалегідь обрахована перевірочна відстань - це так звана *нормальна границя NormBound* [2]: $||s - m_1||^2 + ||t - m_2||^2 \leq NormBound^2$.

Однією з особливостей підписів в ФКП є можливість повного розкриття за допомогою різниці спеціально підібраних підписів: Так в попередніх версіях NSS [1] підписання відбувається по формулі $s = f * w$, де s - це підпис, f - це секретний ключ, а w - це поліном повідомлення. На цей підпис можлива така атака: якщо криптоаналітик може перехопити два підписи s_1 та s_2, то:

$$s_1 - s_2 = f \cdot (w_1 - w_2) = f \cdot 1, \quad (3)$$

де f секретний ключ, а w_1 та w_2 такі повідомлення, що $w_1 - w_2 = 1$. Так поліноми w_i виконують функцію маскування інформації про секретний ключ та виступають у якості сеансових ключів. Схожа практика використання сеансових ключів застосовується і для запобігання атак на NTRU шифрування. Тому головною задачею захисту підпису є підбір таких w_i, щоб $(w_i - w_{i+1})$ різниця була ефективною для маскування f. Тобто, щоб різниця $w_1 - w_2$ не була близькою до одиниці.

На NTRUSign існує атака подібна до тієї атаки, що розглянута вище. Метою даної доповіді є аналіз атаки повного розкриття на NTRUSign такого виду та її ефективності.

Нехай отримано два підписи s_2 та s_1 на одному ключі. Вектори (s_2, t_2) та (s_1, t_1) належать до однієї решітки L, за умови якщо $t_1 = s_1 * h\ mod(q)$ й $t_2 = s_2 * h\ \ mod(q)$. Тоді і різниця цих векторів також належить до цієї решітки. Більш того $s_1 - s_2 = x^k * f$, тобто таким чином з цієї різниці можна отримати секретний ключ f.

Виток секретного ключа відбувається через те, що поліном f має менші коефіцієнти ніж поліном F. Коли підписують представники повідомлення m_1, m_2, то обчислюють:

$$B_1 = \frac{-F*m_1}{q}, b_1 = \frac{f*m_1}{q},\ B_2 = \frac{-F*m_2}{q}, b_2 = \frac{f*m_2}{q}, \quad (4)$$

Якщо m_1, m_2 поліноми, що знаходяться близько один від одного (тобто їх норми мають невелику різницю), тоді поліноми B_1, B_2 відрізняються один від одного а поліноми b_1, b_2 будуть однаковими. Тому різниця підписів є $s_1 - s_2 = f * (B_1 - B_2)$. Таким чином атака буде успішною, якщо $(B_1 - B_2) = 1$. Взагалі, якщо атакуючий зможе отримати s_2 та s_1 від таких спеціально підібраних повідомленнь m_1, m_2, він зможе отримати секретний ключ f. За даними праці [2] вірогідність успішності цієї атаки 1%.

В даній роботі були проведені експерименти, направлені на вивчення стійкості підпису NTRU від вищезгаданої атаки на прикладі реалізації на основі відомої бібліотеки [3]. Досліджуючи вірогідність успішного розкриття випадкового секретного ключа, було отримано кращі результати ефективності атаки. Успішність розкриття ключа залежить від оптимального способу побудови спеціальних повідомлень різниця норм яких є невелике число. В цій роботі запропоновано один з способів побудови, який наведений далі. Для цього створено матрицю I, таку, що $I = M + E$, або $I = M + E'$, де матриця M з тотожними рядками- поліномами повідомлень:

$$M=\begin{pmatrix} m_0 & m_1 & m_2 \\ m_0 & m_1 & m_2 \\ m_0 & m_1 & m_2 \end{pmatrix},\ E = \begin{pmatrix} e & 0 & 0 \\ e & e & 0 \\ e & e & e \end{pmatrix},\ E' = \begin{pmatrix} e & 0 & 0 \\ 0 & e & 0 \\ 0 & 0 & e \end{pmatrix}, \quad (5)$$

а також матриці E, E', в яких рядки це поліноми та e - це маленьке ціле число, e={1, 20}.

Для атаки генерувалася велика сукупність різних незалежних ключів на яких підписували спеціально підібрані повідомлення з матриці I. Потім перевірялося скільки ключів з даної сукупності вдається розкрити вищезгаданим методом. У таблиці міститься вірогідність успіху атаки для виборок ключів із різними довжинами.

Таблиця 1 – Ефективність атаки повного розкриття на NTRUSign.

поліном довжини 157	поліном довжини 439	поліном довжини 743
9 %	8 %	4.8 %

Як видно із таблиці 1 ріст довжини ключа лише лінійно зменшує ефективність атаки.

Хоча саме ця атака не є ефективною при підписі з пертурбаціями, адже B та b будуть складатися із послідовного множення попередніх підписів. Проте ці властивості також могли б відкрити додатковий напрямок для пошуку атак на NTRUSign із пертурбаціями [2].

Таким чином деяка дефектність схеми підписів в ФКП випливає із того, що підпис містить інформацію про секретний ключ, так як підпис - це результат арифметичних операцій в фактор-кільці зрізаних поліномів над многочленами секретного ключа. Так, на відміну від NTRUSign, NTRU шифрування при прямому перетворенні використовує відкритий ключ шифрування. Тобто в NTRU шифруванні секретний ключ не застосовується для отримання шифрограм, які потім передаються каналами зв'язку. І перехоплення цих шифрограм призводить до витоку секретного ключа шифрування не в такій мірі, як це відбувається у випадку із підписом. Для NTRUSign постає більш важка задача: при вироблені підписів потрібно запобігати витоку секретного ключа.

Досліджена в даній роботі атака на основі підібраних повідомлень дає змогу дослідити вразливості підпису до повного розкриття. Застосований метод дозволяє сформувати масив повідомлень, які мають маленькі різниці, що позитивно вплинуло на результати атаки. Перспективним напрямком подальших досліджень є розвиток математичного апарату та методів захисту від вказаних вразливостей.

Список літератури:

1. NSS: The NTRU Signature SchemeNTRU Cryptosystems[Электронный ресурс] / Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, - Режим доступа: http://www/ citeseerx.ist.psu.edu

2. On the NTRU Cryptosystem [Электронный ресурс] / Tommi Meskanen - Режим доступа: tucs.fi/publications/attachment.php?fname=DISS63.pdf

3. http://sourceforge.net /projects/ntru/?source=directory

УДК 003.26:004.056.55

Програмна реалізація блокового симетричного шифру "Калина" з можливістю візуалізації процесів перетворення даних

Штанько В.І. студент 5 курсу

Науковий керівник – Сіденко В.П., старший викладач

Житомирський військовий інститут ім. С.П. Корольова Державного університету телекомунікацій, м. Житомир

В зв'язку зі значними обсягами даних, які циркулюють в інформаційних системах та з урахуванням вимог до їх захисту, виникає необхідність в простих та зручних засобах

захисту. Одним із найбільш поширених засобів захисту є криптографічні алгоритми. Зокрема, для шифрування великих обсягів даних найбільш доцільно використовувати симетричні криптографічні алгоритми.

В якості стандарту блокового симетричного шифрування в Україні використовується алгоритм ГОСТ 28147-89, який введено в дію в 2009. Даний алгоритм володіє певними недоліками, тож було вирішено провести конкурс, за результатами якого був би обраний національний стандарт блокового симетричного шифру.

Одним із учасників конкурсу є криптоалгоритм "Калина", який розроблений на базі стандарту шифрування AES. В порівнянні з AES та ДСТУ ГОСТ 28147:2009 "Калина" має декілька переваг: він простий в реалізації, гнучкий (можливо обирати довжину ключа та блоку даних), підтримує більшу довжину ключа і даних, ніж AES та ГОСТ 28147:2009. Крім того, в БСШ "Калина" покращений алгоритм розгортання ключів, який значно зменшує ймовірність використання слабких ключів.

Однією з ключових проблем, пов'язаних з конкурсом, є проведення криптоаналізу криптоалгоритму "Калина", який би міг підтвердити криптостійкість цього алгоритму. Візуалізація процесів шифрування є одним із варіантів вирішення цієї проблеми, оскільки вона дозволяє на конкретних прикладах прослідкувати яким чином перетворюються дані, визначити вразливі місця шифру тощо.

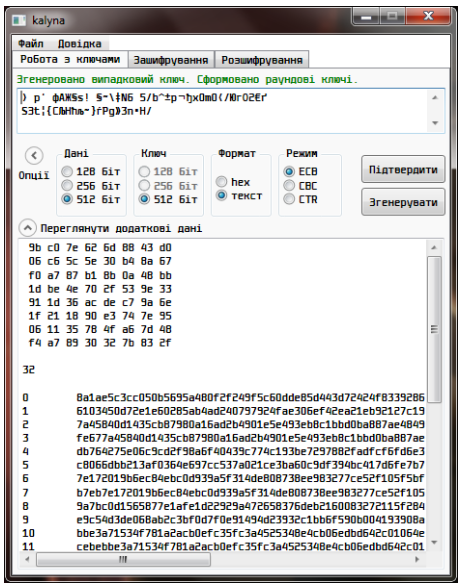

Рисунок 1 - Вікно вибору параметрів алгоритму та роботи з ключами

Саме з цією метою було розроблено програмний засіб, який є реалізацією алгоритму "Калина". Він дозволяє здійснювати шифрування даних різної довжини, яка передбачена специфікацією алгоритму. При цьому можуть використовуватись ключі різної довжини. Дані для обробки можуть вводитися в текстовій формі а також числами шіснадцяткової системи числення (оскільки "Калина" є байт-орієнтованим шифром, така форма даних є зручною для дослідження криптоперетворень). Шифрування даних здійснюється в трьох режимах: ECB (електронна кодова книга) , CBC (зчеплення блоків), а також CTR (режим лічильника). Усі можливі опції, а також приклад ключа і розгорнутих раундових підключів наведені на рисунку 1.

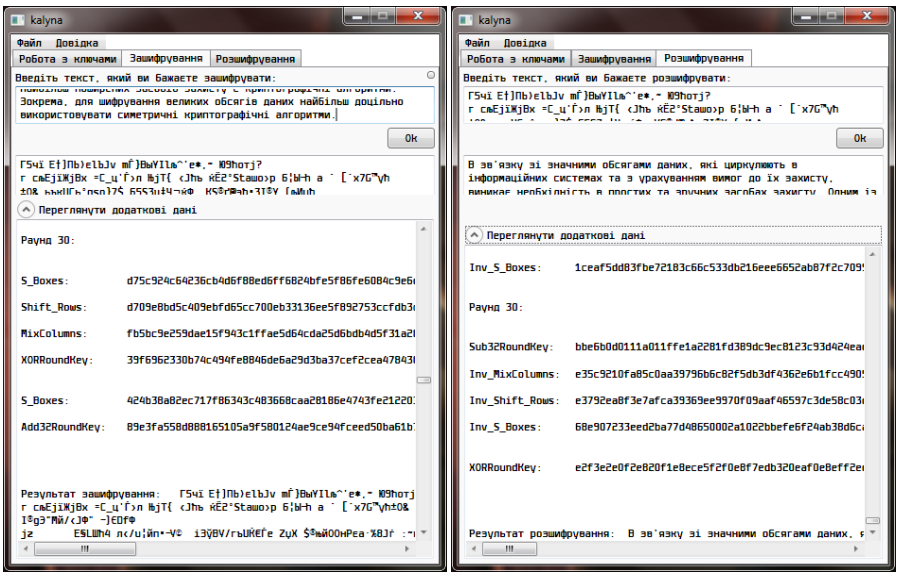

Рисунок 2 - Вікна зашифрування та розшифрування даних

Додаток дозволяє окрім результатів зашифрування та розшифрування переглянути також усі проміжні результати – дані на виході кожного раунду, а також результат кожної елементарної функції, які використовуються в алгоритмі. Маючи результати усіх проміжних перетворень, можна дослідити, яким чином були перетворені дані на тому чи іншому етапі, що є дуже корисним для криптоаналізу алгоритму.

Також додаток можна використовувати в навчальному процесі для наочного пояснення процесів перетворення даних в блокових симетричних шифрах побудованих за принципом SP-мереж.

Список літератури

1. Горбенко, І. Д. Перспективний блоковий симетричний шифр «Калина» : основні положення та специфікації / І. Д. Горбенко, В. І. Долгов, Р. В. Олейніков [та ін.] // Прикладна радіоелектроніка. – 2007. – Т. 6, № 2. – С. 195-208.

2. Єсін В.І. Безпека інформаційних систем і технологій. – Х.: ХНУ імені В.Н. Каразіна, 2013. – 632 с.: ил. / Єсін В.І., Кузнецов О.О., Сорока Л.С.

3. Казіміров А.В. Алгебраїчні властивості схеми розгортання ключів блокового симетричного шифру "Калина". – ХНУРЕ, 2010 - 6 с. / Казіміров А.В., Олєйніков Р.В.

4. Калинин Д. А. Быстродействие шифров «Калина» и AES. / Калинин Д. А., Козина Г. Л. – ЗНТУ, 2013 – 4 с.

Напрямок 5.
Стеганографічні засоби захисту інформації

УДК 004.056.55

Аналіз найбільш поширених алгоритмів ЦВЗ

Будник М.Е., студент 4 курсу
Науковий керівник – Кузнецов О.О., д-р техн. наук, професор
Харківський національний університет імені В.Н.Каразіна, м. Харків

На сьогоднішній день інформаційні технології все більше впливають на наше життя: більшість людей у світі отримають інформацію з різноманітних інтернет-ресурсів та соціальних мереж, які складаються не тільки з текстових статей, а ще й з зображень, відео- та аудіо-файлів. Кожен такий файл був зроблений людиною, яка є автором та власником цієї інформації. Таким чином з'являється необхідність захисту такої інформації від незаконного використання. Рішенням питання захисту інформації в цьому випадку (розглядаючи зображення) є нанесення цифрового водяного знаку.

Цифровий водяний знак (далі - ЦВЗ) – це спеціальні невидимі зміни в зображенні, які приховують в собі деяку інформацію (наприклад інформацію про автора: його ім'я, прізвище тощо).

Кожен алгоритм ЦВЗ характеризується об'ємом прихованої інформації, відсутністю артефактів (видимих змін зображення) та стійкості прихованого контейнера (зазвичай стійкість до стискання) [2].

Одним з таких алгоритмів є алгоритм блокового приховування. Зображення розбивається на блоки, для кожного з яких обчислюється біт парності. Далі відбувається приховування 1 секретного біта повідомлення. Після цього порівнюються біт парності та інформаційний біт, якщо вони різні – змінюємо один з бітів блоку, завдяки чому біт парності та інформаційний біт співпадуть. Найбільшим недоліком цього алгоритму є досить мала стійкість до стискання. Але цей метод має й низку великих переваг: по-перше це можливість зменшення наслідків приховування шляхом збільшення розміру блока, по-друге це можливість модифікації зміненого пікселя в блоці, завдяки чому зміна статистики контейнера буде мінімальною.

Ще одним з алгоритмів ЦВЗ є метод LSB (найменш значущий біт, далі - НЗБ). Колір кожного пікселя залежить від значень інтенсивності кольорів моделі RGB, зазвичай приховування відбувається у найменш чутливий колір для ока людини – синій, саме тому людина не здатна побачити зміни в НЗБ зображення. Основними перевагами цього методу є відносна легкість реалізації алгоритму та досить великий об'єм прихованого контейнера (у деяких випадках можна використовувати одразу 2 НЗБ, таким чином об'єм прихованого контейнера можна подвоїти). Але цей алгоритм також має вагомі недоліки: метод використовується тільки з растровими зображеннями (.gif, .bmp) та має доволі низьку стеганографічну стійкість до атак [3].

Іншим методом є метод псевдовипадкового інтервалу. Суть методу полягає у випадковому розподіленні бітів секретного повідомлення у контейнері, завдяки чому відстань між прихованими бітами визначається псевдовипадково. Цей метод є найбільш ефективним у випадку, коли розмір зображення значно більший за приховуване повідомлення, але вагомим недоліком є відносно невисока стійкість до атаки, через те, що приховані біти розташовано таким самим чином, як і в секретному повідомленні.

Метод псевдовипадкової перестановки більше підходить, якщо контейнер має фіксований розмір. Генератор псевдовипадкових чисел (ПВЧ) створює послідовність індексів (i_1, i_2, …, i_n) та зберігає k-й біт у піксель з індексом i_k. Однак таке зберігання може привести до "перетину", яке з'являється у випадку, коли індекс певного біта контейнера зустрічається більше одного разу у послідовності. "Перетин" здатен спотворити біт, що був вже прихованим у зображення, безумовно це є недоліком алгоритму, але з іншого боку алгоритм здатен показати доволі високий рівень стійкості до різноманітних атак [1].

Для приховування інформації також використовується палітра кольорів, присутніх в зображенні. Такий метод зветься метод зміни палітри. Палітра з N числа кольорів визначається як список пар індексів (I, C_i), який визначає відповідність між індексом і та його вектором кольоровості C_i. При цьому кожен піксель зображення відповідає певному індексу зображення. Оскільки порядок кольорів у палітрі не має значення для вихідного зображення інформація може буде прихована шляхом перестановки кольорів у палітрі. Цей алгоритм не виділяється поміж інших за рахунок стійкості, тому що будь-яка атака, що змінює палітру цілком знищує приховане повідомлення. З іншого боку таке приховування дуже складно відстежити, тому що зображення ніяким чином не змінюється, та насамперед виконується мета стеганографії – приховати факт наявності стеганоконтейнера у зображенні [1].

Одним з досить нетрадиційних алгоритмів є алгоритм, базований на копіюванні блоків однієї випадково обраної текстурної області в іншу, що призводить до появи ідентичних блоків у зображенні. Оскільки копії блоків ідентичні, вони зміняються однаково при перетвореннях самого зображення. Якщо зробити розмір блока досить великим, стійкість до стискання, фільтрації та обертання зображення буде на досить високому рівні. З іншого боку досить вагомим недоліком алгоритму є складність пошуку таких областей, що містять подібні блоки, які можуть бути замінені без вагомої зміни зображення. Також зображення, що підходять для використання цього алгоритму мають бути доволі текстурованими [1].

Усі попередні методи мають спільний недолік – часткове або навіть повне знищення прихованої інформації при стисканні зображення. Більш стійкими алгоритмами до стискання та іншого виду спотворень є методи, що використовують для приховування інформації частотну область контейнера замість просторової.

Найпоширенішими є алгоритми на основі дискретно-косинусного перетворення (ДКП), дискретного перетворення Фурьє (ДПФ), вейвлет-перетворення та інші. Наприклад, алгоритм ДКП є базовим для стандарту JPEG, а вейвлет-перетворення – для JPEG2000 [1]. В алгоритмі JPEG зображення представляється двомірною матрицею N*N, елементи якої складаються з кольорів та яскравості пікселів. Висока ефективність стискання, базується на тому, що в матриці частотних коефіцієнтів, яка утворюється з вихідної матриці, після ДКП низькочастотні компоненти розташовані ближче до верхнього лівого кута, а високочастотні – правого нижнього. Це важливо, тому що більшість графічних образів на екрані складається з низькочастотної інформації, а високочастотну можна загрубити. Після чого ненульові значення низькочастотних компонентів залишаються, у більшій мірі, у лівому верхньому куту матриці. Така матриця кодується з урахуванням повторів нулів. В результаті графічний образ стискається більш ніж на 90 відсотків, при цьому втрати зовсім невеликі тільки на етапі округлення [4].

Список літератури:

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: «МК-Пресс», 2006. —сс. 80 – 113

2. AccessData. Forensic Toolkit product page [Online]. (December 29, 2003).

3. Information Hiding Using Least Significant Bit Steganography and Cryptography [Online]. (June 2012).

4. Information technology – digital compression and coding of continuous-tone still images – requirements and guidelines. (September, 1992).

УДК 004.056

Огляд стеганографічних методів приховування інформації

Гресько Є.І., інженер-системотехнік,
Бабенко В.Г., канд. техн. наук, доцент
Науковий керівник – Фауре Е.В., канд. техн. наук, доцент
Черкаський державний технологічний університет, м. Черкаси

В останні роки у зв'язку з бурхливим розвитком інформаційних технологій та їх широким застосуванням практично у всіх областях людської діяльності все більша увага приділяється засобам захисту інформації. Разом з тим у ряді випадків сучасні криптографічні засоби захисту не повністю задовольняють потребам користувачів, зокрема користувачів глобальних мереж, за вимогами конфіденційності та цілісності. Тому для забезпечення достатнього рівня захисту даних, що передаються, використовують поєднання криптографічних та стеганографічних засобів захисту інформації [1].

Стеганографія є наукою, що забезпечує обмін інформацією таким чином, що приховується сам факт існування секретного зв'язку. Вона не замінює криптографію, а доповнює її ще одним рівнем безпеки. При обробці даних стеганографічними методами відбувається приховування переданої інформації в інших об'єктах (файлах, дисках) таким чином, щоб стороння особа не могла здогадатися про існування прихованого секретного повідомлення. При цьому виявити таке повідомлення досить складно, але якщо це і відбудеться, то для протидії втрати даних повідомлення підлягає зашифруванню на основі криптографічних методів. При реалізації методів стеганографії на комп'ютері (комп'ютерна стеганографія) визначальним фактором є вибір способу кодування даних.

Стеганографію можна умовно розділити на три розділи:

1. Класична стеганографія, яка включає в себе всі «некомп'ютерні методи»;

2. Комп'ютерна стеганографія - напрям класичної стеганографії, що заснований на особливостях комп'ютерної платформи і використанні спеціальних властивостей комп'ютерних форматів даних;

3. Цифрова стеганографія - напрям класичної стеганографії, що заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти, що викликає деякі спотворення цих об'єктів, що не перевищує поріг чутливості середньостатистичної людини. Найчастіше в цих цілях використовується надмірність аудіо- та візуальної інформації [2].

Оскільки цифрова інформація зазвичай передається у вигляді файлів, у комп'ютерній стегосистемі використовуються поняття файл-повідомлення та файл-контейнер. На рисунку 1 представлено загальну модель стеганосистеми [3].

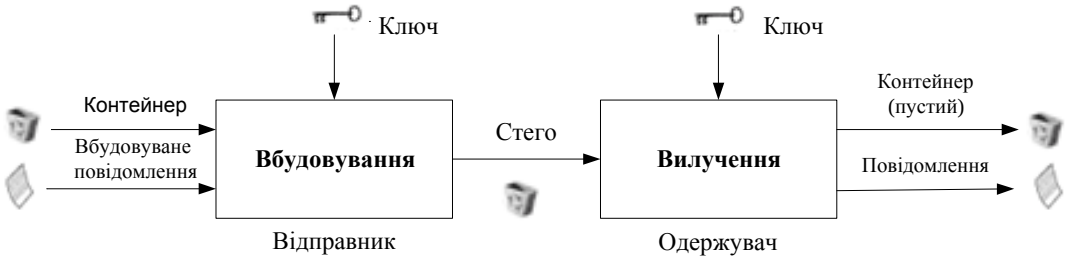

Рисунок 1 – Загальна модель стегосистеми

Основні принципи сучасної комп'ютерної стеганографії можна звести до наступного:

– методи приховування повинні забезпечувати автентичність і цілісність файлу;

– передбачається, що противнику повністю відомі можливі стеганографічні методи;

– безпека методів ґрунтується на збереженні стеганографічним перетворенням основних властивостей переданого файлу по відкритому каналу зв’язку при внесенні до нього секретного повідомлення і деякої невідомої противнику інформації - ключа;

– навіть якщо факт приховування повідомлення став відомий противнику через спільника, вилучення самого секретного повідомлення повинно представляти складну обчислювальну задачу.

В даний час методи комп'ютерної стеганографії розвиваються по двох основних напрямках:

1) методи, засновані на використанні спеціальних властивостей комп'ютерних форматів;

2) методи, засновані на надмірності аудіо та візуальної інформації.

Перший напрямок заснований на використанні спеціальних властивостей комп'ютерних форматів представлення даних, а не на надмірності самих даних. Спеціальні властивості форматів вибираються з урахуванням захисту приховуваного повідомлення від безпосереднього прослуховування, перегляду або прочитання. Дослідивши та проаналізувавши методи першого напрямку зроблено висновок, що всі ці методи прості у користуванні, проте малопродуктивні та забезпечують низький ступінь прихованості. Ці методи призначені тільки для передачі невеликих обсягів інформації [1].

В методах, заснованих на надмірності аудіо та візуальної інформації в якості носія прихованої інформації повинен виступати об'єкт (файл), що допускає спотворення власної інформації, що не порушують його функціональність. Внесені спотворення повинні бути нижче рівня чутливості засобів розпізнавання. В якості носія зазвичай використовуються файли зображень або звукові файли [4]. Такі файли мають велику надмірність і, крім того, зазвичай великі за розміром, забезпечуючи досить місця для приховування простого або форматованого тексту. Приховуване повідомлення може бути простим набором чисел, зображенням, простим або зашифрованим текстом.

Дослідивши та проаналізувавши методи другого напрямку, зроблено висновок, що найбільш поширеним є метод заміни найменш значущих бітів (LSB метод). Основною перевагою цього методу є простота реалізації та можливість таємної передачі великого обсягу інформації. Однак за рахунок введення додаткової інформації спотворюються статистичні характеристики файла-контейнера і приховане повідомлення легко виявити за допомогою статистичних атак. Для зниження компрометуючих ознак потрібне корегування статистичних характеристик. Недоліком методу є також його чутливість до операцій цифрової обробки.

Інші популярні методи вбудовування секретних повідомлень засновані на використанні форматів файлів з втратою даних (наприклад, JPEG). На відміну від LSB методів вони більш стійкі до геометричних перетворень і виявленню каналу передачі. Це досягається за рахунок можливості змінювати якість стислих даних в широкому діапазоні, що призводить до неможливості визначення походження зображення [2].

Актуальність дослідження методів стеганографії невпинно зростає, адже з поширенням персональних комп’ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу великої кількості людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена саме розробці нових та вдосконаленню існуючих методів приховування даних.

У цій роботі розглянуто методи, що використовуються для стеганографічного захисту інформації, виділено їх основні характеристики, переваги й недоліки.

Список літератури

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. - К.: МК-Пресс, 2006. - 288 с.

2. Грибунин В.Г. Цифровая стеганография / В.Г.Грибунин, И.Н. Оков, И.В. Туринцев. - М.: СОЛОН-

Пресс, 2002. - 261с.

3. Генне О.В. Основные положения стеганографии //ООО “Конфидент” журнал “Защита информации. Конфидент”. – 2000. – №3. – С.20-24.

4. Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ [Текст]: учеб. пособие для вузов / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин. – М.: Вузовская книга, 2009. – 220 с.

УДК 004.56

Програмна реалізація приховування даних у нерухомі зображення з використанням дискретного косинусного перетворення елементів контейнерів

Жеревчук А.П. студент 5 курсу
Науковий керівник – Сіденко В.П., старший викладач
Житомирський військовий інститут ім. С.П. Корольова Державного університету телекомунікацій, м. Житомир

Стеганографічну систему можна описати як класичну систему передачі даних, що містить передавач, приймач даних та середовище передачі (для стеганосистем – контейнер) [1]. У якості контейнера можливо використовувати текст, зображення, аудіофайл чи відеозапис. В силу багатьох причин (відносно великий обсяг цифрового представлення зображень, фіксований розмір контейнера, наявність у більшості зображень текстурних областей з шумовою структурою, слабка чутливість людського ока до незначних змін параметрів зображення, розвинуті методи цифрової обробки зображень тощо) більшість стеганографічних методів використовує у якості контейнерів графічні файли.

Практичний інтерес становить питання ефективності стеганосистеми за наявності у каналі атаки компресії. Найбільш стійкими до атак компресії виступають методи приховування даних, що розглядають контейнер не в просторовій, а у частотній області. Зокрема показано, що найбільш доцільним є приховування даних у смузі із середніми частотами, де шуми є мінімальними. Низькочастотні субсмуги містять переважну частину енергії зображення, високочастотні субсмуги найбільшим чином піддаються впливові з боку різноманітних алгоритмів обробки, як то компресія чи фільтрація.

Серед багатьох методів частотної декомпозиції зображень існує практична доцільність застосування дискретного косинусного перетворення (ДКП). Дане перетворення використовується у алгоритмі обробки графічних зображень JPEG, що на сьогодні є найбільш поширеним алгоритмом обробки графічних файлів [2]. Одним з варіантів приховування даних є відносна заміна величин коефіцієнтів ДКП. При використанні методу забезпечується низька щільність приховування – один біт даних на 64 пікселі контейнеру, що сприяє підвищенню прихованості даних.

Нехай C – первинне зображення (контейнер-оригінал), M – повідомлення, що підлягає приховуванню. Тоді модифіковане зображення (стеганоконтейнер) $S = C + M$. Модифіковане зображення S візуально нерозрізнене з первинним і може бути піддано у стеганоканалі компресії із втратами: $S' = \theta(S)$, де $\theta(\bullet)$ – оператор компресії. Завдання одержувача – видобути з одержаного контейнера S' вбудовані на попередньому етапі біти даних M. Основне питання, на яке необхідно дати відповідь, полягає у пошуку пропускної здатності прихованого каналу передачі даних за умови наявності у каналі зв’язку певного алгоритму компресії. Повідомлення M передається по каналу, що має два джерела "шуму": C – зображення-контейнер і "шум" θ, що виникає в результаті операцій компресії/декомпресії. S' та M' - можливо спотворені стеганоконтейнер і, як результат, повідомлення. Структурну

схему стеганосистеми представлено на рис. 1.

Недоліком даного методу є невеликий простір ключів (обмежена кількість коефіцієнтів ДКП), що не дозволяє гарантувати повну безпеку даних. Для вирішення даної проблеми запропоновано попередньо зашифровувати вбудовувані дані блоковим симетричним алгоритмом, наприклад AES. Також доцільно змінювати коефіцієнти при вбудовуванні кожного наступного біту даних користуючись генератором псевдовипадкової послідовності. Окремо слід наголосити на важливості коректної реалізації запропонованого методу, оскільки на даному етапі можливо внести у контейнер спотворення, що негативно впливають на прихованість даних. Також важливо обрати коректні значення матриці квантування, що забезпечуватимуть оптимальний компроміс між прихованістю даних та їх стійкістю до компресії.

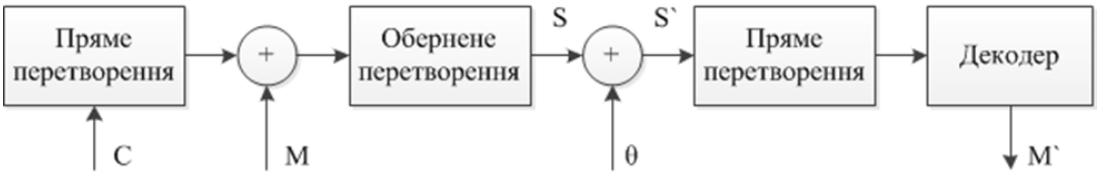

Рисунок 1 – Структурна схема стеганосистеми за наявності в стеганоканалі атаки компресії

З метою імплементації описаних вище ідей було створено інтерактивну програму, що реалізує приховування файлів даних, із забезпеченням їх конфіденційності шляхом зашифровування блоковим симетричним алгоритмом AES з довжиною ключа 256 біт у режимі CTR, у нерухомі зображення методом заміни величин коефіцієнтів ДКП з візуалізацією процесів.

Спроектована стеганосистема є стійкою до атак компресії, забезпечує збереження конфіденційності даних за допомогою шифрування блоковим симетричним шифром AES у режимі CTR.

Розроблена програма являє собою головне вікно, в якому розміщено елементи інтерфейсу програми. Функціональне наповнення програми згруповано за допомогою вкладок користувацького інтерфейсу. Перелічимо компоненти інтерфейсної частини програми:

- вкладка "Вбудовування даних" (рис. 2);
- вкладка "Покроковий перегляд" при вбудовуванні даних (рис. 3);
- вкладка "Вилучення даних" (рис. 4);
- вкладка "Покроковий перегляд" при вилученні даних (рис. 5).

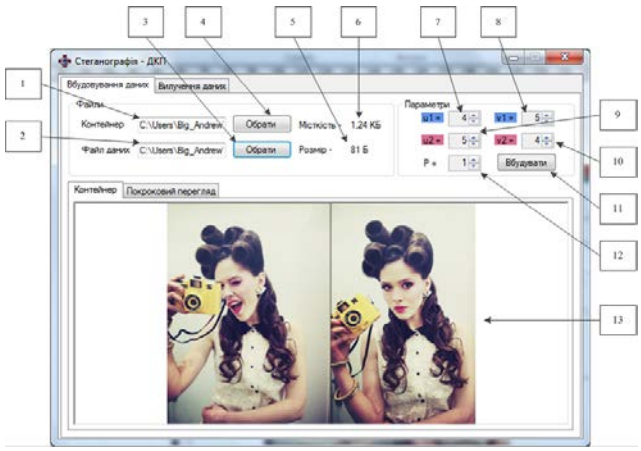

Рисунок 2 – Вкладка "Вбудовування даних"

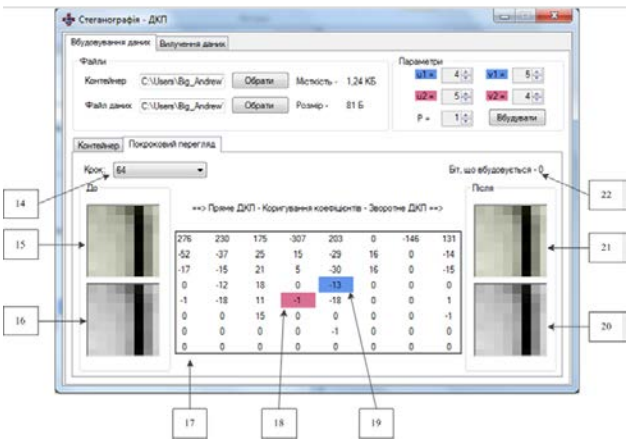

Рисунок 3 – Вкладка "Покроковий перегляд" при вбудовуванні даних

Для початку процесу вбудовування даних необхідно використовуючи кнопки 3 та 4 обрати контейнер для вбудовування даних та файл, що буде вбудовано. Зображення

обраного контейнеру буде показано у полі 13. Після цього обрати значення коефіцієнтів, що будуть використовуватись для приховування даних за допомогою елементів управління 7, 8, 9 та 10. Також необхідно обрати значення порогу для вбудовування даних за допомогою елемента 12. Після проведення даних налаштувань натискаємо кнопку 11. У діалоговому вікні необхідно обрати місце зберігання та ім'я файлу заповненого контейнера. Після проведених операції програма вбудовує дані у зображення та зберігає заповнений контейнер на диск. Результати вбудовування можна переглянути покроково на відповідній вкладці. Обираючи за допомогою списку 14 крок вбудовування можна переглянути значення вбудовуваного біту, значення матриці коефіцієнтів ДКП, операцію, що здійснюється над коефіцієнтами.

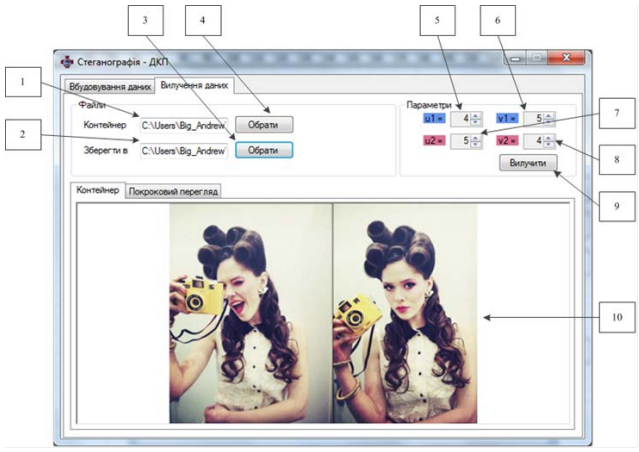

Рисунок 4 – Вкладка "Вилучення даних"

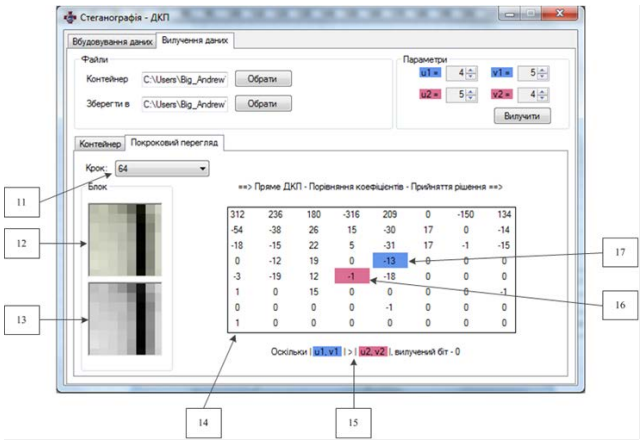

Рисунок 5 – Вкладка "Покроковий перегляд" при вилученні даних

На дану програмну реалізацію отримане свідоцтво про реєстрацію авторського права на твір у Державної служби інтелектуальної власності України від 05.11.2014 № 58276 "Програма приховування даних у нерухомі зображення методом заміни величин коефіцієнтів дискретного косинусного перетворення з візуалізацією процесів".

Список літератури

1. Цифровая стеганография / Оков И. Н., Грибунин В. Г., Туринцев И. В. и др.; Под ред. В. Г. Грибунина. – М.: Солон-Пресс, 2002. – 272 с.

2. Швідченко І. В. Стійкі криптостеганографічні алгоритми / І. В. Швідченко // Искусственный интеллект. – 2009. - №1. – с. 218 – 226.

УДК 004.056.55

Стеганографическая защита информации с использованием 3D-печати

Кузнецов А.А., д-р техн. наук, профессор,
Коваленко О.Ю. студент 4 курса
Харьковский национальный университет им. В.Н. Каразина, г. Харьков

Стеганографическая защита предполагает сокрытие не только смыслового содержания, но и самого факта существования информационных данных [1 – 3]. Наиболее часто методы стеганографии используются для скрытной передачи различных информационных сообщений, для защиты авторского права, обеспечения подлинности и аутентичности посредством создания цифровых водяных знаков, скрытного встраивания

идентификационных номеров, кодов подлинности, информирующих заголовков и пр.

В данной работе предлагается комплекс стеганографической защиты, в котором информационные данные скрываются в процессе послойного создания (выращивания) твердотельного объекта при использовании различных технологий 3D-печати. Основная идея проекта состоит во встраивании (стеганографическом кодировании) информационных данных в цифровую 3D-модель, по которой в последующем послойно создается (распечатывается) твердый объект (готовое изделие или прототип для дальнейшей доводки). Процесс встраивания (стеганографического кодирования) реализуется с использованием секретных ключевых данных, что исключает несанкционированный доступ к защищаемой информации, нарушение ее целостности, аутентичности и конфиденциальности. Кроме того, применяемая стеганографическая защита не снижает эксплуатационных, эстетических и прочих иных свойств готового изделия, поскольку технологии, применяемые для нанесения слоев, не модифицируются. Таким образом, предлагаемый комплекс инвариантен способу послойного выращивания, т.е. может комплектоваться произвольными периферийными устройствами 3D-печати различных фирм изготовителей с любыми доступными материалами и принципами послойного создания.

Процесс извлечения встроенных данных осуществляется посредством сканирования полученного твердого тела. Извлеченные сканером данные подвергаются стеганографическому декодированию с использованием секретных ключевых данных. На этом этапе обеспечиваются различные услуги безопасности, например, целостность, аутентичность, причастность (неотпирательство), конфиденциальность. Для повышения достоверности (помехоустойчивости) встраиваемые данные дополнительно подвергаются избыточному кодированию, которое позволяет с заданной вероятностью обнаруживать и/или исправлять возникшие в процессе послойной печати/сканирования ошибки. Предлагаемый комплекс предлагается использовать в различных областях. Например, для скрытной передачи информационных сообщений с обеспечением различных услуг безопасности (целостности, аутентичности, причастности, конфиденциальности и пр.). Удаление, искажение или модификация встроенных данных невозможны без физического разрушения готового изделия, т.е. предлагаемый комплекс идеально подходит для обеспечения подлинности послойно выращенных изделий, защиты их от несанкционированного копирования и недобросовестных подделок, обеспечения авторского права.

Список літератури

1. Конахович Г.Ф., Пузиренко О.Ю. Компьютерная стеганография. – К.: «МК-Пресс», 2006.– 288 с.
2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.
3. Хорошко В.А., Шелест М.Е. Введение в компьютерную стеганографию. – К., 2002. – 140 с.
4. Кузнецов О. О., Євсеєв С. П., Король О. Г. Стеганографія. Х.: Вид. ХНЕУ, 2011. – 232 с.

УДК 004.056.55

Стеганографічний метод приховування даних в аудіозаписі на основі прямого розширення спектру

Федоров О.В., аспірант денної форми навчання
Науковий керівник – Кузнєцов О.О., д-р техн. наук, професор
Харківський національний радіотехнічний університет, м. Харків

Одним з перспективних напрямків розвитку сучасної стеганографії є методи приховування даних в аудіо записах на основі використання складних дискретних сигналів.

У роботах [1,2] було показано, що використання технології прямого розширення спектру дозволяє, використовуючи розвинений математичний апарат цифрової обробки

сигналів, реалізувати стеганографічне приховування інформації в аудіо записах. При цьому кожний блок m_i інформаційного повідомлення приховується в окремому блоці контейнера (аудіо запису) C_i.

В результаті, для кожного інформаційного блоку m_i формується модульований інформаційний сигнал:

$$E_i(t) = \sum_{j=0}^{M-1} m_{ij}(t)\Phi_j, \quad (1)$$

де $m_{ij}(t)$ – інформаційний сигнал, що відповідає j-му біту та і-му блоку інформаційного повідомлення,

$$m_{ij}(t) = \begin{cases} +1, m_{ij} = 1; \\ -1, m_{ij} = 0; \end{cases} \quad (2)$$

$\Phi_j = (\varphi_{j0}, \varphi_{j1}, \ldots, \varphi_{jn-1})$ – розширюючий кодовий сигнал довжини n з множини слабокорельованих одна з одною псевдовипадкових послідовностей (ПСП) $\Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\}$,

$$\Phi_{iz} = \begin{cases} +1 \\ -1 \end{cases}, \ z = 0, \ldots, n-1, \quad (3)$$

M – число біт в одному блоці інформаційного повідомлення, тобто число інформаційних біт, що приховуються в окремий блок контейнера аудіо файлу C_i. Величина M характеризує, таким чином, пропускну здатність Q = M/N стеганоканалу передачі інформації, де N – об'єм блоку контейнера аудіо файлу C_i.

Формула (1) демонструє процес модуляції інформаційних сигналів $m_{ij}(t)$ розширюючими сигналами Φ_j, що традиційно використовуються у системах зв'язку з прямим розширенням спектру. Оскільки отриманий кодовий сигнал за своїми статистичними показниками схожий на шум, то отриманий широкополосний сигнал $E_i(t)$ тяжко відрізнити від шуму в каналі зв'язку, що і дозволяє здійснити приховану передачу. Таким чином, повідомлення в каналі зв'язку сприймаються як шум, і за рахунок великої потужності ансамблю сигналів Φ і прямого розширення спектру забезпечується висока скритність каналу зв'язку.

Для приховування інформаційного повідомлення в контейнер сформований сигнал $E_i(t)$ побітно додають до блоку контейнера C_i:

$$S_i = C_i + E_i \cdot G, \quad (4)$$

де G > 0 – коефіцієнт підсилення розширюючого сигналу, що визначає «енергію» біт m_{ij}, j = 0, ..., n - 1 інформаційної послідовності, що приховуються. Стеганограма (заповнений контейнер) S формується за допомогою з'єднання окремих блоків S_i.

При зворотному перетворені даних первинний контейнер C і його окремі блоки C_i на прийомній стороні не потребуються. Операція декодування відбувається за допомогою відтворення схованого повідомлення шляхом проектування кожного блоку S_i отриманої стеганограми S на всі $\Phi_j \in \Phi$. Щоб здійснити зворотне перетворення j-й біт повідомлення з і-го блоку аудіо запису S_i необхідно визначити коефіцієнт кореляції між Φ_j і прийнятим блоком S_i:

$$\rho(S_i, \Phi_j) = \frac{1}{n}\sum_{z=0}^{n-1} S_{iz}\Phi_{jz} = G \cdot \frac{1}{n}\sum_{z=0}^{n-1} E_{iz}\Phi_{jz} + \frac{1}{n}\sum_{z=0}^{n-1} C_{iz}\Phi_{jz} \quad (5)$$

Якщо масив C_i було сформовано випадковим чином і рівновірогідним процесом, тоді другий доданок у правій частині виразу (4) близький до нуля і ним можна знехтувати. Внаслідок, маємо:

$$\rho(S_i, \Phi_j) \approx G \cdot E_i \cdot \Phi_j = G \cdot \sum_{l=0}^{M-1} m_{il}(t)\Phi_l\Phi_j = G \cdot \sum_{l=0}^{M-1} m_{il}(t)\sum_{z=0}^{n-1}\Phi_{lz}\Phi_{jz} \quad (6)$$

Усі послідовності з множини Ф за визначенням слабокорельовані, тобто при $l \neq j$ маємо $\rho(\Phi_i, \Phi_j) \approx 0$. Внаслідок цього, усіма доданками у правій частині рівняння (5) при $l \neq j$ можна знехтувати. Звідси маємо:

$$\rho\left(S_i, \Phi_j\right) \approx G \cdot m_{ij}(t) \cdot \frac{1}{n} \sum_{z=0}^{n-1} \left(\Phi_{jz}\right)^2 = G \cdot m_{ij}(t) \quad (7)$$

Тоді значення $m_{ij}(t)$ можуть бути легко відтворені за допомогою виразу:

$$m_{ij}(t) = \begin{cases} +1, \text{при } \rho\left(S_i, \Phi_j\right) \approx G; \\ -1, \text{при } \rho\left(S_i, \Phi_j\right) \approx -G. \end{cases} \quad (8)$$

де знак «≈» допускає наявність незначного статистичного взаємозв'язку окремих елементів множини Ф і C_i. Така стеганосистема отримує усі переваги широкополосних систем зв'язку з прямим розширенням спектру: стійкість до несанкціонованого вилучення схованого повідомлення, стійкість до знищення і модифікації приховуваного повідомлення.

Таким чином, використання технології прямого розширення спектру дозволяє здійснити приховування інформації в аудіо записах, і здійснити таким чином стеганографічний захист [3].

Список літератури

1. W.Bender, D. Gruhl, N.Morimoto, A.Lu, Techniques for Data Hiding. IBM Systems Journal, 35(3&4): pp. 313-336, 1996

2. P. Bassia, I. Pitas, Robust Audio Watermaking In The Time Domain // Department of Informatics, University of Thessalonica (http://poseidon.csd.auth.gr/voyatzis/creus.zip)

3. Конахович Г.Ф., Пузиренко А.Ю. Комп'ютерна стеганографії. Теорія і практика. – К.: «МК-Пресс», 2006. – 288 с., іл.

УДК 004.056.55

Стеганозахист з використанням файлових систем зберігання даних на флеш-накопичувачах

Фесенко Д.О., студент 4 курсу
Науковий керівник – Кузнецов О.О., д-р техн. наук, професор
Харківський національний університет імені В.Н.Каразіна, м. Харків

Вступ

Безпека зберігання та передачі конфіденційної інформації є дуже важливим напрямком розвитку сучасних інформаційних технологій. Традиційно секретна інформація шифрується з використанням криптостійкіх алгоритмів, однак, в деяких сценаріях використання шифрування даних за допомогою криптографічних методів недостатньо. Факт існування зашифрованої інформації з використанням криптографічних методів досить легко можна виявити. Стеганографія може вирішити цю проблему.

У даній роботі досліджуються методи стеганозахисту, які засновані на використанні файлових систем зберігання даних на флеш-накопичувачах.

Особливості зберігання даних на флеш-накопичувачах та методи стеганозахисту

Нові технології приховування інформації використовують особливості файлових систем та кластерного зберігання даних, що дозволяє надійно захищати їх від третьої сторони [1 - 3]. Файлова система – це певний порядок організації та модифікацій інформації на носіях у комп'ютерних системах або в іншому цифровому обладнанні. Саме файлова система визначає формат та спосіб фізичного зберігання інформації, які звичайний користувач бачить як файл певного типу (аудіо, фото, відео або текстовий документ) [4 - 6].

Твердотільні носії, такі, як флеш-диски, своїм інтерфейсом даних схожі на звичайні

жорсткі диски, але мають свої проблеми і недоліки. Вони потребують особливої обробки такими алгоритмами як вирівнювання зносу і виявлення та виправлення помилок.

До файлових систем для флеш-дисків (твердотільних носіїв) відносять: FAT - початково дискова файлова система - тепер часто використовується на флеш-дисках (має обмеження на розмір файлу в 4 гігабайти); ExFAT - розширена версія FAT, використовувана для флеш-дисків та запатентована Microsoft, часто називається як FAT64 - обмеження 2^{64} байт (16 ексабайт); TFAT - транзакційна версія FAT файлової системи; FFS2 - продовження файлової системи FFS1, одна з ранніх файлових систем для флеш-карт, розроблена і запатентована Microsoft на початку 1990х років; JFFS - оригінальна лог-структурована Linux файлова система для NOR-флеш-носіїв; JFFS2 - продовження JFFS для NAND- і NOR-флеш-носіїв; LogFS - призначена для заміни JFFS2, краща розширюваність; Non-Volatile File System - файлова система для флеш-дисків, розроблена Palm, Inc.; YAFFS – файлова система, призначена для NAND-флеш, але може використовуватися в NOR-флеш-дисках.

Усі відомі стеганографічні методи приховування даних в файлових системах використовують випадкові дані, записані в різні «невикористовувані» місця файлової системи, які легко виявити третьою стороною, відповідно, у цього метода є тільки властивість правдоподібного заперечення. Хасаном Ханом [2, 3] був запропонований метод двох прихованих каналів, який забезпечує правдоподібне заперечення і призначений для зберігання конфіденційної інформації в файловій системі. Ці методи не вимагають ніякої додаткової інформації для запису на диск. Вони приховують інформацію за допомогою спеціального розподілу дискового простору (блоків або кластерів), що містять нешкідливі, так звані «покриваючі файли» або cover-файли.

Обидва методи використовують один coverfile. Секретне повідомлення в двійковому вигляді вбудовується за допомогою особливості розподілу кластерів coverfile в файловій системі. Перший спосіб застосовує властивість фрагментації файлів в якості носія. Кластер кожного файлу, починаючи з другого, в файловій системі FAT може бути поруч з попереднім кластером (нефрагментований) або, якщо наступний кластер зайнятий, він може бути в іншому місці на диску (фрагментований). Біти секретного повідомлення послідовно приховані розподілом фрагментованих або нефрагментованих кластерів. Друга методика, представлена в [2, 3], ґрунтується на такому підході: повідомлення розділене на дрібні деталі і ці частини, інтерпретовані як натуральні числа, потім кожне число виражається відстанню між фрагментованими кластерами coverfile. У такому випадку ємність прихованого каналу збільшується в порівнянні з першим методом, але алгоритм вбудовування даних більш складний.

Сутність реалізованого методу та його оцінка

Основна ідея методу вбудовування даних [7], що реалізується у даній роботі, полягає в тому, щоб використовувати кілька coverfile і приховати секретне повідомлення за допомогою відносних позицій кластерів цих файлів один щодо одного. У такому випадку ігноруються всі інші файли в файловій системі, і тільки кластери, що належать всім coverfiles аналізуються.

За допомогою цієї стратегії можна вбудувати більше, ніж один біт секретного повідомлення в один кластер файлової системи. У такому випадку, імена coverfiles стають секретним ключем, тому що приймаюча сторона повинна знати імена і точний порядок цих файлів для того, щоб успішно зчитувати приховане повідомлення.

В ході досліджень було реалізовано досліджуваний алгоритм на мові C++. Проведено експерименти дослідження можливостей приховування даних у кластерних файлових систем на флеш-накопичувачах. Розглянутий метод приховування даних в кластерних файлових системах з використанням декількох coverfiles дуже простий в реалізації. На відміну від двох аналогічних методів, це не створює ніяких колізій під час операції, так що інші файли на диску не повинні бути порушеними під час вбудовування даних, що збільшує швидкість роботи.

Досліджений метод приховування даних вимагає, щоб секретний ключ служив для відновлення даних; це дає додатковий рівень безпеки для прихованих даних, викликаючи багаторівневу властивість правдоподібного заперечення (plausible deniability). Метод не передбачає додаткової інформації, і всі об'єкти файлової системи повністю відповідають стандартам (тобто FAT32), таким чином, прихована інформація є стійкою до загальних дискових модифікацій (регулярне редагування файлу, видалення, створення, і т.д.). З іншого боку, деякі низькорівневі інструменти (такі як утиліти дефрагментації) можуть змінити розміщення coverfiles і знищити приховані дані.

Висновки

Ефективність запропонованого способу не залежить від розміру файлової системи або вільного простору на диску. Пропонований метод приховування даних приводить до фрагментації файлової системи і створює переплетення файлів. Наприкінці можна сказати, що пропонований метод приховування даних має властивість подвійного правдоподібного заперечення.

Список літератури

1. A. Czeskis, D.J. S. Hilaire, K. Koscher, S. D. Gribble, T. Kohno, B. Schneier. Defeating encrypted and deniable file systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications. HotSec, 2008, pp. 1–7.

2. H. Khan, M. Javed, S. A. Khayam, F. Mirza. Designing a cluster-based covert channel to evade disk investigation and forensics. Computers & Security, 2011, Vol. 30, 35–49.

3. Hassan Khan, Mobin Javed, Fauzan Mirza. Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel. National University of Science & Technology (NUST), Islamabad 44000, Pakistan.

4. B. Carrier. File system forensic analysis. Addison-Wesley Professional, 2005.

5. A. D. McDonald, M. G. Kuhn. StegFS: a steganogra-phic file system for Linux. Information Hiding, 1999, Vol. 1768, 462–477.

6. E. Huebner, D. Bem, C. K. Wee. Data hiding in the NTFS file system. Digital Investigation, 2006, Vol. 3, 211–226.

7. Nerijus Morkevičius, Grigas Petraitis, Algimantas Venčkauskas, Jonas Čeponis. Covert Channel for Cluster-based File Systems Using Multiple Cover Files. Information technology and control, 2013, Vol.42, No.3.

УДК 004.056.55

Аналіз та порівняльні дослідження методів технічної стеганографії

Швагер А.С., студентка 4 курсу
Науковий керівник – Кузнецов О.О., д-р техн. наук, професор
Харківський національний університет імені В.Н.Каразіна, м. Харків

У сучасному світі практично не існує людини, яка б не знала або хоча б не чула про комп'ютерні технології. Інформація - це серце XXI століття і тому вона потребує захисту. Стеганографія - наука, здатна приховати не приховуючи. Технічна стеганографія - новий розділ сучасної цифрової стеганографії. В її завдання входить вивчення методів і засобів вбудовування та вилучення інформаційних повідомлень в різні контейнери, однак, з використанням технічних особливостей передачі, зберігання і модифікацій. Яскравим прикладом є стеганографічні методи, які реалізуються за допомогою файлових систем.

Файлова система – це певний порядок організації та модифікацій інформації на носіях у комп’ютерних системах або в іншому цифровому обладнанні. Саме файлова система визначає формат та спосіб фізичного зберігання інформації, які звичайний користувач бачить як файл певного типу (аудіо, фото, відео або текстовий документ). Різноманіття файлових систем дозволяє реалізовувати певний ряд задач. Кожна із існуючих систем має обмеження

на споживання власних ресурсів: максимальний розмір файлів та розділів, сукупність атрибутів файлів. Деякі файлові системи надають можливість розмежування доступу або шифрування даних, так звані сервісні можливості.

Файлова система встановлює, де та яким чином буде існувати файл на фізичному носії. Одиницею файлової системи є кластер. Кластер – логічна одиниця зберігання даних у таблиці розміщення файлів. Ця одиниця поєднує в собі групу секторів доріжки і зазвичай є найменшою одиницею, що може бути виділена для запису та зберігання даних. Термін «кластер» у широкому своєму значенні використовується, коли мова йде про такі файлові системи як FAT (File Allocation Table) та NTFS (New Technology File System) компанії Microsoft Windows. Інші існуючі файлові системи мають схожі визначення: зони, блоки.

На сьогоднішній день, зазначена вище файлова система FAT є найбільш розповсюдженою та доступною, як для користувачів так і для розробників. Можливо, саме тому її використовують для експериментів та досліджень стеганографічних завдань. Чотири версії системи FAT (FAT8, FAT12, FAT16, FAT32) дозволяють задовольнити будь-які вимоги для реалізації задач. Різниця полягає в тому, що кожна з версій має власну розрядність записів у дисковій структурі. Кажучи простіше – кожна версія визначає кількість біт, які будуть зберігати номер кластера.

NTFS – файлова система, що повільно витісняє FAT. Особливістю системи є використання спеціалізованих структур даних для зберігання інформації, що в свою чергу підвищує надійність, продуктивність та ефективність використання дискового простору. NTFS зберігає дані, а саме інформацію про файли, у головній таблиці MFT (Master File Tablet). Однак поряд з усіма перевагами цієї файлової системи є суттєвий недолік – специфікації не знаходяться у відкритому доступі, що дуже ускладнює реалізацію методів технічної стеганографій.

Проблематика приховування даних у файлових системах обговорювалася вже не раз в різній літературі. При цьому були помітні явні мінуси методів, такі як: розробка спеціальної файлової системи [1], очевидність вбудовування [2, 3], або ж занадто узагальнена інформація [4, 5]. У деяких статтях пропонували удосконалення існуючих методів [6, 7].

Хасан Хан [8, 9] запропонував використання двох прихованих каналів, які забезпечують принцип правдоподібного заперечення. Особливістю стало те, що метод не вимагає додаткової інформації. Приховування відбувається за рахунок спеціального розподілу дискового простору одиниць (блоки, кластери), що містяться в cover-файлах.

Суть методу - вбудовування реального двійкового повідомлення за допомогою розподілу кластерів cover-файлів в системі FAT.

Одне рішення - використання принципу фрагментації, але при цьому виникає проблема вже існуючих записів. Тобто накладання інформації у вже зайнятий кластер.

Друге рішення - поділ повідомлення на дрібні підповідомлення, які інтерпретуються як натуральні числа. Кожне натуральне число виражається як відстань між фрагментованими кластерами.

Явною перевагою другого рішення запропонованого алгоритму є можливість збільшення ємності прихованого каналу, але алгоритм вбудовування даних є більш складним для програмної реалізації. Також не можна промовчати про те, що при використанні другого рішення методу - ігноруються всі інші файли у файловій системі. Аналізу піддаються лише кластери свідомо відомих файлів. Метод дозволяє вбудовувати більш, ніж 1 біт секретного повідомлення в один кластер файлової системи, а імена cover файлів – це секретні ключі усієї нехитрої стеганографічної системи. Для успішного вилучення необхідно знати точні імена та порядок файлів. Явище файлового переплетіння (спеціального типу фрагментації) дозволяє забезпечити додатковий рівень безпеки.

Розглядаючи даний метод технічної стеганографії [10], як потенційно сприйнятний для масового використання, слід враховувати, що вбудована інформація є стійкою до будь-яких модифікацій третіми особами. Однак існує загроза ненавмисного видалення -

наприклад, програми для дефрагментації. Також існує ризик перерозподілу кластерів дискового простору, що уявляє собою неконтрольовану загрозу схованій інформації. Окрім того слід враховувати той факт, що фрагментація знижує продуктивність алгоритму. Це значить, що метод має змогу на подальший розвиток та вдосконалення.

Список літератури:

1. R. J. Anderson, R. M. Needham, A. Shamir. The steganographic file system. In: Proceedings of the Second International Workshop on Information Hiding, London, UK, 1998, pp. 73–82.

2. A. Czeskis, D.J. S. Hilaire, K. Koscher, S. D. Gribble, T. Kohno, B. Schneier. Defeating encrypted and deniable file systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications. HotSec, 2008, pp. 1–7.

3. K. Eckstein, M. Jahnke. Data hiding in journaling file systems. In: Refereed Proceedings of the 5th Annual Digital Forensic Research Workshop, New Orleans, Louisiana, USA, 2005, pp. 1–8.

4. E. Huebner, D. Bem, C. K. Wee. Data hiding in the NTFS file system. Digital Investigation, 2006, Vol. 3, 211–226.

5. S. Piper, M. Davis, G. Manes, S. Shenoi. Detecting hidden data in ext2/ext3 file systems. IFIP Int. Conf. Digital Forensics, 2005, 245–256.

6. A. D. McDonald, M. G. Kuhn. StegFS: a steganogra-phic file system for Linux. Information Hiding, 1999, Vol. 1768, 462–477.

7. H. Pang, K. L. Tan, X. Zhou. StegFS: a steganogra-phic file system. In: Proceedings of the 19th International Conference on Data Engineering, 2003, Vol. 1, pp. 657–668.

8. H. Khan, M. Javed, S. A. Khayam, F. Mirza. Designing a cluster-based covert channel to evade disk investigation and forensics. Computers & Security, 2011, Vol. 30, 35–49.

9. Hassan Khan, Mobin Javed, Fauzan Mirza. Evading Disk Investigation and Forensics using a Cluster-Based Covert Channel. National University of Science & Technology (NUST), Islamabad 44000, Pakistan.

10. Nerijus Morkevičius, Grigas Petraitis, Algimantas Venčkauskas, Jonas Čeponis. Covert Channel for Cluster-based File Systems Using Multiple Cover Files. Information technology and control, 2013, Vol.42, No.3.

Напрямок 6.
Технічні засоби захисту інформації

УДК 004.056.55

Система пассивной защиты от лазерных микрофонов на основе уголковых отражателей

Беденко Д.А., студент 5 курса,
Мудров Д.Э, студент 5 курса
Научный руководитель – Заболотный В.И., канд. техн. наук, доцент
Харьковский национальный университет радиоэлектроники, г. Харьков

Эффективность любой лазерной системы акустической разведки зависит от параметров лазера, детектора, используемых в установке, от параметров среды, внешних условий функционирования системы (погодные условия, запылённость воздушной среды и т.д.). Данная система рассматривает съем информации с оконного стекла. Рассмотрим принципы функционирования разработанной системы.

Прежде всего, для работы рассмотренной системы защиты необходимо совместное размещение лазера и детектора. В современных системах данная ситуация проблемой не является, т.к. лазер и микрофон в большинстве случаев располагаются в одном помещении для обеспечения скорости и простоты настройки системы. Это происходит по той причине, что при разнесении детектора и лазера подготовка системы требует значительных усилий и не всегда является возможной ввиду, например, невозможности размещения детектора в точке, куда приходит промодулированное вибрирующим под действием голоса стеклом излучение [1, 2].

Вторым важным элементом разработанной системы защиты является использование трёхгранных уголковых отражателей, основной особенностью которых является отражение приходящего сигнала в направлении, по которому сигнал пришел. Таким образом, учитывая совместное расположение лазера и детектора в современных системах лазерной разведки, теоретически возможным является создание помехи по мощности на детекторе системы разведки путём отражения на детектор части луча лазера, которая не является информативной, а проникает сквозь стекло в помещение. Рассмотрим особенности функционирования разрабатываемой системы защиты.

Для трёхгранного уголкового отражателя с треугольными гранями мощность отраженного сигнала будет равна [3]:

$$P_1 = \sigma_1 * p_1, \quad (1)$$

где σ_1 – эффективная площадь рассеивания (ЭПР) уголкового отражателя; p_1 – плотность потока мощности падающей волны; P_1 – мощность излучения, отраженного уголковым отражателем.

ЭПР, в свою очередь, зависит от длины облучающей волны и геометрических размеров отражателя:

$$\sigma_1 = \frac{4\pi}{3\lambda^2} a^4, \quad (2)$$

где α – длина ребра уголкового отражателя; λ – длина падающей волны.

Мощность сигнала, принятого на вход фотодетектора после его отражения от оконного стекла, определяется по формуле:

$$P_2 = \frac{p_2 S_A k \sigma_2}{R^2}, \quad (3)$$

где $p_2 -$ плотность потока мощности падающей волны; S_A – площадь поверхности объектива детектора; k - коэффициент пропускания принимающей оптической системы; σ_2 – эффективная площадь рассеивания (ЭПР) стекла; R – расстояние от «лазерного микрофона» до оконного стекла; P_2 – мощность модулированного вибрирующим окном лазерного луча на приемнике ЛСАР.

ЭПР стекла в данном случае рассчитывается как:

$$\sigma_2 = S k_u \xi, \quad (4)$$

где S – коэффициент пропорциональности, количественно характеризующий степень рассеивания лазерного луча при попадании на стекло; k_u – коэффициент направленного воздействия стекла, который характеризует степень концентрации мощности лазерного излучения, которое рассеивается стеклом в сторону детектора ЛСАР; ξ – коэффициент деполяризации лазерного излучения в момент отражения от стекла.

Для достижения искомой защиты необходимым является выполнение условия $P_1 > P_2$.

В результате анализа технических характеристик современных ЛСАР было установлено, что даже самые современные из данных систем имеют расходимость луча не менее 0,5 мрад. Общепринятый диаметр линзы лазера d = 0,5÷1 см, но это не мешает использовать для создания шума гармоники ненулевого порядка. Такой вывод был сделан в результате анализа характеристик существующих на текущий день ЛСАР. На практике это означает, что полное попадание пятна лазерного луча на поверхность уголкового отражателя не является необходимым для создания модулированной помехи, а наличие у отражателей относительно высокого ЭПР позволяет уменьшить их размеры и разнести в пространстве.

В результате анализа технических характеристик современных ЛСАР было установлено, что даже самые современные из данных систем имеют расходимость луча не менее 0,5 мрад. Общепринятая ширина лазера (диаметр линзы лазера) d = 0,5÷1 см.

Для подсчета диаметра проекции луча лазера на стекле смоделируем ситуацию разведки с расстояния 100 метров, диаметр линзы лазера 0,005м, угол расхождения 0,5мрад. Такие параметры являются наименее неблагоприятными для ведения защиты. Таким образом, область расхождения луча находится как:

$$D' = \tan \alpha * L = \tan 0{,}0285 * 100 = 0{,}05\text{м}. \quad (5)$$

D – диаметр проекции луча лазера на поверхности стекла.

d – диаметр луча (линзы) лазера.

L – расстояние от источника лазерного излучения до поверхности вибрирующего стекла.

D' – область расхождения луча лазера.

α – угол расхождения луча.

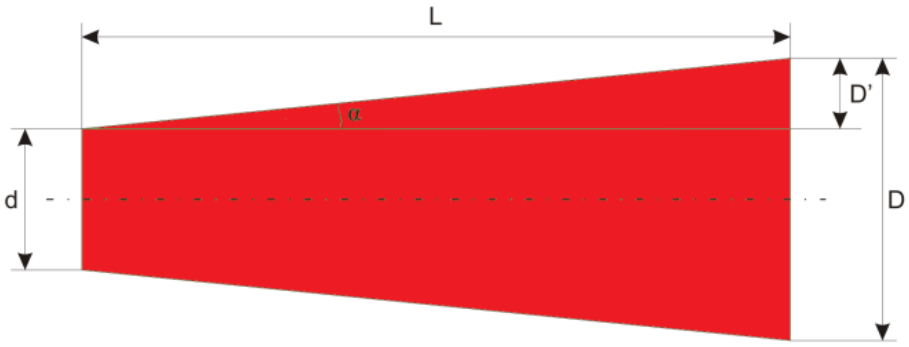

Рисунок 1 – Схема расхождения луча лазера

Учитывая ширину лазерного пучка и область расхождения луча лазера, на расстоянии 100 метров от источника излучения лазерное пятно на поверхности стекла будет иметь диаметр 10,5см.

Еще одним важным элементом системы является стекло. Оконное стекло является почти прозрачным для ближнего инфракрасного излучения (до 2,5мкм), в диапазоне частот которого работают современные ЛСАР. Коэффициент отражения для стекла рассчитывается по формуле:

$$r = \left(\frac{n-1}{n+1}\right)^2, \tag{6}$$

где n – показатель преломления оптического материала, и для стекла в общем случае он равен 1,5. Таким образом, стекло отражает лишь 4% падающего излучения.

Согласно формулам 1 - 4 и необходимому условию обеспечения защиты $P_1 > P_2$ можно определить необходимое условие как:

$$\frac{4\pi}{3\lambda^2} a^4 p_1 > \frac{p_2 S_A k S k_u \xi}{R^2}. \tag{7}$$

Согласно формуле 6 стекло отражает лишь 4% падающего на него излучения. Для максимизации нежелательного с точки зрения защиты варианта примем условие, что на фотодетектор ЛСАР попадает все 100% отраженного и промодулированного стеклом излучения. В реальных условиях стекло имеет микротрещины и неровности, воздушная среда содержит пыль и другие частицы, которые существенно ослабляют мощность и изменяют направление отражения луча лазера.

Проанализировав формулы 1, 2, 7 можно прийти к выводу, что мощность отраженного сигнала пропорционально увеличивается с увеличением площади пятна от луча лазера на поверхности стекла. Таким образом, если стекло пропускает до 96% падающего излучения (не учитывая излучения, задержанного самим стеклом), необходимо, чтобы уголковый отражатель отражал чуть более 4,5% падающего на стекло излучения, что на практике позволит использовать несколько относительно небольших отражателей, разнесенных на определенное расстояние друг от друга.

Список литературы

[1] Лазерные микрофоны - универсальное средство разведки или очередное поветрие моды? [Электронний ресурс] / Инженерно-производственное предприятие "НЕРА-С". – Режим доступа: http://www.nera-s.com/publication/301/ - 21.05.2014.

[2] А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков Технические средства и методы защиты информации [Текст]: учебное пособие для ВУЗов. – Москва: Машиностроение, 2009. – 508с.

[3] Эффективная площадь рассеяния - Физический смысл ЭПР [Электронний ресурс] / Вся авиация. От сверхлегких самолетов до бизнес-джетов. – Режим доступа: http://www.vonovke.ru/s/effektivnaya_ploschad_rasseyaniya_-_fizicheskiy_smyisl_epr – 11.09.2014.

УДК 681.5.004

Взаємна декомпозиція символів в шифрувальних пристроях

Бурмістров С.В., аспірант
Науковий керівник – Кочкарьов Ю.О., д. т. н, професор, Рудницький В.М., д. т. н, професор
Черкаський державний технологічний університет, м. Черкаси

Одними із найбільш розповсюджених шифрувальних пристроїв (ШП) є апарати, призначені для посимвольного кодування інформації. Активна промислова реалізація даних пристроїв почалася ще до появи електронних пристроїв в 20-х роках минулого століття [1]. Принцип роботи даних пристроїв полягає в тому, що під час кодування інформації один символ заміняється на інший із використовуваного обмеженого алфавіту (див. табл.1) [2]. Функції $\left\{f_1^{\arg}, f_2^{\arg},..., f_n^{\arg}\right\}$ називаються функціями кодування (ФК). Набір ФК визначає поточний фіксований ключ (ПФК). Для алфавіту, заданому *n*-розрядними машинними кодами (МК), оптимальним значенням ПФК є *n* ФК, серед яких немає двох однакових. Розрядність ФК становить 2^n біт.

Таблиця 1

Один із варіантів кодування інформації за допомогою поточного фіксованого ключа

Початковий символ	**Бінарний код початкового символу**			**Бінарний код передаваємого символу**			**Кодований символ**
$a_0^{\arg}$	0	0	0	0	1	1	$a_0^{in} = a_3^{\arg}$
$a_1^{\arg}$	0	0	1	1	1	0	$a_1^{in} = a_6^{\arg}$
$a_2^{\arg}$	0	1	0	0	0	1	$a_2^{in} = a_1^{\arg}$
$a_3^{\arg}$	0	1	1	1	1	1	$a_3^{in} = a_7^{\arg}$
$a_4^{\arg}$	1	0	0	0	1	0	$a_4^{in} = a_2^{\arg}$
$a_5^{\arg}$	1	0	1	0	0	0	$a_5^{in} = a_0^{\arg}$
$a_6^{\arg}$	1	1	0	1	0	0	$a_6^{in} = a_4^{\arg}$
$a_7^{\arg}$	1	1	1	1	0	1	$a_7^{in} = a_5^{\arg}$
	$\uparrow$ $f_3^{\arg}$	$\uparrow$ $f_2^{\arg}$	$\uparrow$ $f_1^{\arg}$	$\uparrow$ f_1^{in}	$\uparrow$ f_2^{in}	$\uparrow$ f_3^{in}	
	Початкові функції аргументів			**Функції кодування**			

Постановка проблеми. Даний спосіб кодування є найбільш ефективним в сучасних комерційних мережах у випадку використання для кожного наступного передаваємого МК нового ПФК. Але навіть в такому випадку він має 2 суттєві недоліки, що знижують його можливості:

1. Під час кодування символ заміняється на символ. Тому незакодоване і закодоване сповіщення має однакову кількість символів, що спрощує процес несанкціонованого розкодування інформації.

2. Функцією кодування можуть бути лише МК, що мають в коді однакову кількість нулів і одиниць. Тому кількість можливих варіантів ПФК становить $n! < 2^n$, що значно менше від кількості МК вказаної розрядності

Метою даної роботи є розробка додаткового блоку ШП, розміщеного послідовно за ШП, що дає змогу робити передаваємий текст «гумовим» (текст, в якому кількість передаваємих символів може варіюватись відносно кількості символів первинного тексту) та суттєво збільшити кількість можливих комбінацій шифрування тексту.

Принцип роботи додаткового блоку ШП ґрунтується на розкладанні передаваємих кодів на частини (декомпозиція МК) та наступному їх склеюванні із різних МК. Нехай дано послідовність передаваємих МК $\{a_5^{in}, a_9^{in}, a_7^{in}, a_3^{in}, a_{11}^{in}, a_{13}^{in}\}$. Якщо синхронно зсунути певні біти в даній послідовності (див. табл. 2), отримують закодоване сповіщення, що по довжині зростає від 1 до *n* символів (*n* - розрядність МК). При цьому є можливість інверсувати будь-який із бітів МК. В таблиці 2 під значком «*» слід розуміти довільний випадково вибраний біт.

Таблиця 2

Один із варіантів кодування інформації за допомогою взаємної декомпозиції символів

№ пп	Передаваємий символ	Машинний код передаваємого символа до кодування	Машинний код передаваємого символа після кодування
1	a_5^{in}	$a_{05.7}^{in}a_{05.6}^{in}a_{05.5}^{in}a_{05.4}^{in}a_{05.3}^{in}a_{05.2}^{in}a_{05.1}^{in}a_{05.0}^{in}$	$\tilde{a}_{05.7}^{in} * \tilde{a}_{05.5}^{in} ** \tilde{a}_{05.2}^{in} \tilde{a}_{05.1}^{in} \tilde{a}_{05.0}^{in}$
2	a_9^{in}	$a_{09.7}^{in}a_{09.6}^{in}a_{09.5}^{in}a_{09.4}^{in}a_{09.3}^{in}a_{09.2}^{in}a_{09.1}^{in}a_{09.0}^{in}$	$\tilde{a}_{09.7}^{in} \tilde{a}_{05.6}^{in} \tilde{a}_{09.5}^{in} ** \tilde{a}_{09.2}^{in} \tilde{a}_{09.1}^{in} \tilde{a}_{09.0}^{in}$
3	a_7^{in}	$a_{07.7}^{in}a_{07.6}^{in}a_{07.5}^{in}a_{07.4}^{in}a_{07.3}^{in}a_{07.2}^{in}a_{07.1}^{in}a_{07.0}^{in}$	$\tilde{a}_{07.7}^{in} \tilde{a}_{09.6}^{in} \tilde{a}_{07.5}^{in} * \tilde{a}_{05.3}^{in} \tilde{a}_{07.2}^{in} \tilde{a}_{07.1}^{in} \tilde{a}_{07.0}^{in}$
4	a_3^{in}	$a_{03.7}^{in}a_{03.6}^{in}a_{03.5}^{in}a_{03.4}^{in}a_{03.3}^{in}a_{03.2}^{in}a_{03.1}^{in}a_{03.0}^{in}$	$\tilde{a}_{03.7}^{in} \tilde{a}_{07.6}^{in} \tilde{a}_{03.5}^{in} \tilde{a}_{05.4}^{in} \tilde{a}_{09.3}^{in} \tilde{a}_{03.2}^{in} \tilde{a}_{03.1}^{in} \tilde{a}_{03.0}^{in}$
5	a_{11}^{in}	$a_{11.7}^{in}a_{11.6}^{in}a_{11.5}^{in}a_{11.4}^{in}a_{11.3}^{in}a_{11.2}^{in}a_{11.1}^{in}a_{11.0}^{in}$	$\tilde{a}_{11.7}^{in} \tilde{a}_{03.6}^{in} \tilde{a}_{11.5}^{in} \tilde{a}_{09.4}^{in} \tilde{a}_{07.3}^{in} \tilde{a}_{11.2}^{in} \tilde{a}_{11.1}^{in} \tilde{a}_{11.0}^{in}$
6	a_{13}^{in}	$a_{13.7}^{in}a_{13.6}^{in}a_{13.5}^{in}a_{13.4}^{in}a_{13.3}^{in}a_{13.2}^{in}a_{13.1}^{in}a_{13.0}^{in}$	$\tilde{a}_{13.7}^{in} \tilde{a}_{11.6}^{in} \tilde{a}_{13.5}^{in} \tilde{a}_{07.4}^{in} \tilde{a}_{03.3}^{in} \tilde{a}_{13.2}^{in} \tilde{a}_{13.1}^{in} \tilde{a}_{13.0}^{in}$
7	-	-	$* \tilde{a}_{13.6}^{in} * \tilde{a}_{03.4}^{in} \tilde{a}_{11.3}^{in} ***$
8	-	-	$*** \tilde{a}_{11.4}^{in} \tilde{a}_{13.3}^{in} ***$
9	-	-	$*** \tilde{a}_{13.4}^{in} ****$

Апаратна реалізація даного блоку здійснюється на синхронних RS-трігерах. Трігери розміщенні каскадом, щоб була можливість зберігати в пам'яті до *n* послідовних символів сповіщення. В трігерах використовуються як прямі так і інверсні виходи

Перевагами даного кодування є:

1. Новий спосіб кодування, що не залежить від інших видів кодування. Тому він може використовуватись комплексно з іншими видами кодування.
2. Початковий і закодований текст мають різну кількість символів, що затрудняє процес розкодування.
3. Кількість варіантів кодування становить $2^n \cdot (n! \cdot (n-1)! \cdot (n-2)! \cdot \ldots \cdot 1!)!$, де *n* – розрядність МК.

Список літератури

1. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. / М.В.Адаменко. – М: ДМК-Пресс., – 2012. – 256 с.

2. Криптографическое кодирование: коллективная монография / под редакцией В.Н. Рудницкого, В.Я. Мильчевича. – Харьков: из-во ООО «Щедрая усадьба плюс», 2014. -240 с.

УДК 004.056.55

Дослідження спектрів симетричних сигналів

Перепадя В.І., студентка 4 курсу
Науковий керівник – Заболотний В.І., канд. техн. наук, доцент
Харківський національний університет радіоелектроніки, м. Харків

На основі аналізу рішень рівнянь Максвелла, показана зміна форми відгуку наведених значень е.р.с. в антені розвідувального пристрою в дальній зоні каналу ПЕМВ. Встановлено, що форма е.р.с. для електричної антени відповідає другій похідній вихідного сигналу, а для магнітної - третій. Використовуючи властивості перетворень Фур'є, були визначені спектральні функції розвіданих сигналів. Показана можливість визначення величин параметрів вихідних сигналів по значенням виміряних «нулів» спектра ПЕМВ.

В даній роботі будуть розглянуті та досліджені спектральні функції одиночного імпульсу симетричної форми. Такі імпульси формують зображення на екрані монітору. Практика показала, що монітор електронно-променевої трубки (ЕПТ) створює найбільш потужні ПЕМВ небезпечних сигналів.

З числа найбільш інформативних сигналів в ЕОМ слід зазначити дискретні сигнали. По-перше, вони являються одними з найпотужніших; по-друге, послідовними в часі; по-третє, періодично повторюються багато разів, зберігаючи високу стабільність у часі. Фронт і спад імпульсів мають кінцеву протяжність, яка визначається інерційними параметрами каскадів відеопідсилювачів сигналів. Для зменшення видимих спотворень зображення на екрані, конструктори моніторів прагнуть зробити форму фронту і спаду симетричною і як можна коротшою.

Зазначене вище, дає підставу запропонувати в якості першої моделі сигналу трапецеїдальний імпульс тривалістю τ по рівню половини амплітуди A. Протяжність фронту і спаду - Δ. Такі сигнали (рис. 1) характерні для потужних вихідних ключових каскадів відеопідсилювачів. В якості другої моделі можна вибрати сигнал з косинусквадратичною формою фронту і спаду. В телевізійній техніці такі сигнали апроксимували перехід сходинки контрастного зображення круглим зчитувальним променем. Тривалість переходу – δ.

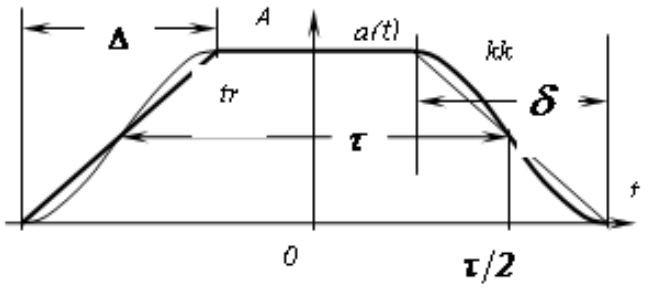

Рисунок 1 – Сигнали моделі ТКВІ: *tr* – трапецеїдальний; *kk* – з косинус квадратичними фронтом и спадом.

Слід зазначити, що вибір початку координат по середині імпульсу дозволяє спростити отримання кінцевих виразів, не впливаючи на зміст результатів. Для спрощення знаходження спектральних функції сигналів слід скористатися відомими властивостями Фур'є - перетворень [3], що зв'язують часові та частотні функції сигналів: при зсуві в часі, диференціюванні та інтегруванні , додаванні .

Проаналізувавши все вищезгадане і провівши деякі розрахунки, можна зробити висновок:

– $A\tau$ характеризує інтенсивність спектральної функції на низьких ($\omega \to 0$) частотах. При постійній амплітуді A, що характерно для зображень символів і тексту на екрані, інтенсивність низьких частот залежить від тривалості інформаційного сигналу;

– На більш високих частотах вплив тривалості імпульсу на спектральні функції незначний.

– Фронти імпульсів - Δ і δ не більш протяжні ніж мінімальне значення його тривалості τ. При їх нульовому значенні формули перетворюються в спектральні функції прямокутних імпульсів;

– На високих частотах проявляється дія фронтів. Їх подовження призводить до зниження рівня спектральних складових.

Список літератури

1. Заболотный В.И., Емельянова Ю.В., Муромцева Н.А. статья Модель технического канала утечки информации за счёт побочных электромагнитных излучений монитора // Прикладная радиоэлектроника. 2007. № 6. – С. 33-37.

2. Гольдштейн Л.Д., Зернов Н.В. Электромагнитные поля и волны. М.: Изд. «Советское радио». – 1971. – 664с.

3. Харкевич А.А.. Спектры и анализ. 4-е узд. М.: Гос. Изд. Физмат. литературы. – 1962. – 236с.

УДК 004.62

Дослідження використання хешування в програмі оптимізації системи контролю технологічного процесу та вибір оптимального методу

Шувалова Л.А., канд. техн. наук, доцент,
Білас І.І., магістрант
Черкаський державний технологічний університет, м. Черкаси

Використання хешування в програмі оптимізації системи контролю технологічного процесу зумовлено вимогою забезпечення імітозахисту (захисту від нав'язування хибних даних зловмисником під час перехоплення інформаційного повідомлення у відкритому каналі зв'язку).

В загальному випадку *хешування* (hashing) – це перетворення за визначеним алгоритмом вхідного масиву даних довільної довжини в вихідний бітовий рядок фіксованої довжини.

Хешування застосовується для побудови асоціативних масивів, пошуку дублікатів в серіях наборів даних, побудови досить унікальних ідентифікаторів для наборів даних, підрахунок контрольних сум з метою виявлення випадкових або навмисних помилок при зберіганні або передачі, для зберігання паролів в системах захисту (в цьому випадку доступ до області пам'яті, де знаходяться паролі, не дозволяє відновити сам пароль), при виробленні електронного підпису (на практиці часто підписується не саме повідомлення, а його хеш-образ), для імітозахисту тощо.

Безпосередньо для захисту від фальсифікації переданої інформації хешування проводиться криптостійкою функцією над повідомленням, об'єднаним з ключем, відомим тільки відправнику і одержувачу повідомлення. Таким чином, криптоаналітик не зможе

відновити код за перехопленим повідомленням і значенням хеш-функції, тобто, не зможе підробити повідомлення [1].

Особливістю використання хешування у якості імітозахисту для даної задачі в архіваторі системи контролю технологічного процесу є те, що у якості ключа з яким об'єднане повідомлення використовується відкритий ключ RSA, який доступний як у відповідального за продукції бригадира зміни (відправник) з одного боку, так і в контролюючих органах (одержувач) з іншого, але при цьому тримається у секреті від зловмисника. При цьому, отримане повідомлення разом з хешем використовується також для ідентифікації відправника одержувачем.

В зв'язку із зазначеним, для забезпечення імітозахисту для даної задачі доцільно використовувати хешування MD5 (Message Digest 5).

MD5 – це популярний 128-бітний алгоритм хешування, розроблений професором Рональдом Л. Рівестом в 1991 році. Він призначений для створення «відбитків» або «дайджестів» повідомлень довільної довжини. Прийшов на зміну MD4, що був недосконалим.

Переваги використання цього алгоритму у вигляді насамперед доступності реалізації зумовленою популярністю та поширеністю, а також відносною швидкістю виконання, перекривають наявні недоліки, які не є критичними.

Список літератури

1. Фергюсон Н., Шнайер Б. Практическая криптография. – М.: Диалектика, 2004. – 432 с.

Напрямок 7.
Комплексні системи захисту інформації

УДК 004.342.75:004.352.65

Методика розподілу доступу до ресурсів системи управління авіатранспортним комплексом з забезпеченням захисту інформації

Козловський В.В., д-р техн. наук, професор,
Міщенко А.В., канд. техн. наук, професор,
Васянович В.В., аспірант
Національний авіаційний університет, м. Київ

Вступ Сьогодні в авіатранспортному комплексі України функціонують аналогові вузли (ВСС). Дані вузли виробили свій ресурс і в найближчий час повинні бути демонтовані. Новітня цифрова комутаційна техніка і комп'ютерні технології дозволяють значно поширити можливості вузлів, ввести на локальних телефонних мережах інтелектуальні послуги й організувати додаткові довідкові, інформаційні і замовні служби, зробити їх більш привабливими для користувачів і більш надійними з точки зору інформаційної безпеки. Дані вузли спецслужб захисту інформації в авіатранспортній сфері стануть міцним фундаментом в забезпеченні інформаційної безпеки авіатранспортного комплексу.

Бурхливий розвиток мережі Інтернет і технології пакетної передачі даних вчинив безпосередній вплив на структуру розподілу доступу до ресурсів інформаційних систем. У підсумку з'явився мультимедійний Центр обслуговування інформаційних систем (ММ ЦОІС). Сучасний ММ ЦОІС – це інтегроване прикладне середовище, на базі якої здійснюється управління всіма видами електронної взаємодії з користувачами через телефонну мережу та мережу Інтернет. В ЦОІС відбувається конвергенція традиційної технології комутації каналів і нової технології пакетної передачі інформації. Обмін повідомленнями з абонентами ЦОІС здійснюється через телефонну мережу (мовні і факсимільні повідомлення) та через Інтернет (текстові повідомлення чат, текстові, музичні і мовні повідомлення електронної пошти, мовні повідомлення IP-телефонії).

Основна частина

Фундамент оперативного управління комплексною системою захисту інформації в АТК складається з двох компонентів: інформаційної та програмної складової.

Інформаційне забезпечення – найважливіший компонент ЦОВ (ClCn). Воно повинне реалізовуватися у виді відповідних баз даних (БД) сучасної архітектури. Більшість ЦОВ (ClCn) використовують архітектуру реляційних БД.

При виборі СКБД для рішення визначеної задачі варто враховувати:

– вид служби, для якої створюється база даних, і число РМ в службі;

– локальна чи розподілена структура створюваної мережі;

– зміст інформації, що передбачається зберігати;

– показники вартості;

– необхідну продуктивність, час відповіді системи на еталонне питання;

– вимоги надійності.

Для невеликих локальних мереж можна рекомендувати MS SQL Server у середовищі OS Windows XP Professional, для більш великих мереж краще застосувати Oracle у середовищі OS Windows XP Professional чи в середовищі OS Unix, для розподілених мереж можливе застосування DB2 у середовищі OS Windows XP Professional чи в середовищі OS Unix. Остаточний вибір варіанта реалізації СКБД повинний відбуватися на стадії проектування конкретного ЦОВ (ClCn). При розробці і створенні бази даних необхідно провести аналіз змісту інформації, що передбачається зберігати: інформація предметної області, довідкова інформація, описи абонентів і т.д. На підставі аналізу варто розробити:

– схему бази даних, враховуючі всі збережені сутності і їхні взаємозв'язки;

– індекси для пошуку інформації зі змісту;

– екранні представлення і форми;

– збережені процедури і тригери;

– процедури резервного копіювання і відновлення;

– процедури архівації;

– різні SQL-сценарії для взаємодії з базою даних (запити, адміністрування, збір статистики і т.д.);

– групи користувачів;

– міри забезпечення безпеки шляхом надання різним групам користувачів різних прав доступу до бази даних.

Для нормального функціонування створена база даних вимагає постійного адміністрування і рішення наступних задач:

– створення облікових записів користувачів і керування ними;

– створення ролей, сервісних правил, прав доступу;

– забезпечення захисту даних у мережі;

– навчання і підтримка користувачів;

– модернізація існуючого програмного забезпечення й установка нового;

– архівація даних;

– імпорт і експорт даних;

– попередження втрат даних;

– моніторинг вільного простору для збереження даних на сервері;

– настроювання продуктивності й оптимізація;

– протоколювання бази даних;

– резервне копіювання даних;

– відновлення даних після аварії;

– захист мережі від вірусів;

– діагностика;

– модернізація і заміна компонентів мережі;

– додавання в мережу нових робочих станцій.

Для первісного введення інформації з неелектронних носіїв повинні бути передбачені сучасні системи оптичного розпізнавання тексту (OCR). Отриману в електронному виді вихідну інформацію необхідно перетворити в структури обраної бази даних. Для цього необхідна розробка відповідного програмного забезпечення, що враховує предметну область БД. Сформована база даних повинна бути перевірена на несуперечність програмним способом, відповідна програма також повинна бути розроблена.

Для пошуку інформації зі змістом необхідно створити повнотекстовий індекс – алфавітний покажчик слів, що зустрічаються в тексті. Для роботи з документами на

російській або українській мові повинний бути спеціально адаптований сервіс повнотекстового індексу англомовної універсальної СКБД. Важливим для ефективної роботи пошукової системи є створення словника стоп-слів.

Для підтримки інформації бази даних в актуальному стані вона повинна постійно коректуватися. Можливі наступні способи внесення коректур у БД:

– операторами служби, локально чи дистанційно;

– власником інформації, локально чи дистанційно;

– автоматично програмним забезпеченням ЦОВ (ClCn) на підставі аналізу зовнішніх джерел інформації;

– комбінованим способом, що охоплює перераховані вище способи.

Доступ до інформації бази даних повинні мати система інтерактивної мовної відповіді IVR, оператори, начальник зміни, адміністратор служби, адміністратор ЦОВ. Для роботи оператора необхідно розробити зручні екранні форми для видачі запитів до БД і відображення на екрані отриманої інформації. Повинна також передбачатися можливість віддаленого доступу до бази даних.

Програмне забезпечення разом з апаратними засобами повинне забезпечити функціональні вимоги, пропоновані до ЦОВ (ClCn) у дійсних технічних вимогах, з урахуванням загальних вимог.Програмне забезпечення ЦОВ (ClCn) повинне містити наступні компоненти прикладного і сервісного програмного забезпечення:

– програмне забезпечення для керування системою ACD;

– програмне забезпечення для керування системою IVR;

– інформаційне програмне забезпечення;

– програмне забезпечення системи контролю і реєстрації;

– програмні засоби розробки додатків.

Програмне забезпечення для керування системою ACD призначено для спостереження за роботою системи, оскільки сама система лише керує розподілом викликів між операторами за встановленими правилами і не показує, як вона функціонує. Дане ПО повинно мати наступні можливості:

– видавати звіти про якість обслуговування викликів, що надходять, і про роботу операторів у реальному масштабі часу і за задані проміжки часу;

– мати модульну структуру і дозволяти швидке нарощування системи ACD;

– інтегруватися з іншими додатками (облік викликів, розподіл витрат, визначення послідовності робіт і т.д.);

– забезпечувати гнучкість системи, підтримуючи важливі для користувача параметри.

Інформаційне програмне забезпечення призначене для одержання з інформаційного сховища ЦОВ (ClCn) даних, необхідних для обслуговування абонента. Воно повинне включати мережну інформаційну базу даних (NID) і сервісні логічні програми (SLP), що відповідають за виконання різних видів обслуговування. Інформаційна база даних повинна містити параметри маршрутів установлення з'єднання, історію звертань кожного абонента (при необхідності), довідкову інформацію, статистичну інформацію про роботу ЦОВ.

Висновки

Аргументовано подальший розвиток методу оперативного управління комплексної системи захисту інформації авіатранспортного комплексу, що відрізняється від відомих економічно обґрунтованим підходом до вирішення оптимізаційних задач розміщення та управління ресурсами та дозволяє в загальному аналізувати і здійснювати управління інформаційною безпекою авіатранспортного комплексу. Удосконалено методику розподілу доступу до ресурсів обробки і управління запитами в комп'ютеризованих інформаційних системах авіатранспортного комплексу, яка відрізняється від відомих комплексним

використанням контактних сценаріїв управління інформаційними ресурсами підприємства, що дозволяє контролювати процес обміну даними і підвищити безпеку інформаційних ресурсів систем обробки та управління запитами.

Список літератури

1. Качинський А.Б. Безпека, загрози, ризик. Наукові концепції та математичні методи. Інститут проблем національної безпеки. Національна академія служби безпеки України. Київ, 2004. – 470 с.

2. Косарів О.Й. Інформаційні системи на транспорті / О.Й. Косарів, А.М. Мержвинська. – К.: НАУ, 2001.

3. Самарский А.А. Гулин А.В. Численные методы. М: "Наука" 1989г. – 432с.

4. Кулинич, А. А. Субъектно-ориентированная сис-тема концептуального моделирования «Канва» [Текст]: матер. 1-й межд. конф. / А. А. Кулинич // Когнитивный ана-лиз и управление развитием ситуаций. – Москва, 2001. – С. 348.

5. Томас, Р. В., Френд Д. Х., ДаСильва Л. А., МакКензи А.Б. Когнитивные сети: адаптация и обучение для достижения конечных запланированных показателей [Текст] / Р. В. Томас, Д. Х. Френд, Л. А. ДаСильва, А. Б. МакКензи //Журнал IEEE Communications.3. – 2006. –No 12, Вип. 44. – С. 21. 2001.

6. Цибульский В. Р., Фомин В. В. Когнитология. Основные понятия когнитивного управления // Вестник кибернетики. Вып. 1.– Тюмень: Изд-во ИПОС СО РАН, 2002.– С. 34 – 37.

УДК 681.322.067

Етапи та принципи створення комплексної системи захисту інформації

Куницька С.Ю., канд. техн. наук, доцент
Черкаський державний технологічний університет, м. Черкаси

Система захисту інформації повинна створюватися спільно із створюваною комп'ютерною системою. При побудові системи захисту можуть використовуватися існуючі засоби захисту або ж вони розробляються спеціально для конкретної КС. Залежно від особливостей комп'ютерної системи, умов її експлуатації і вимог до захисту інформації процес створення КСЗІ може не містити окремих етапів, а також утримання їх може дещо відрізнятися від загальноприйнятих норм при розробці складних апаратно-програмних систем. Розробка систем включає наступні етапи:

- розробка технічного завдання;
- ескізне проектування;
- технічне проектування;
- робоче проектування;
- виробництво дослідного зразка.

Процес розробки систем, що закінчується виробленням технічного завдання, називають науково-дослідною розробкою, а іншу частину роботи по створенню складної системи називають дослідно-конструкторською розробкою. Дослідно-конструкторська розробка апаратно-програмних засобів ведеться із застосуванням систем автоматизації проектування, алгоритми проектування добре вивчені і відпрацьовані. Тому особливий інтерес представляє розгляд процесу науково-дослідного проектування.

Науково-дослідна розробка КСЗІ

Метою цього етапу є розробка технічного завдання для проектування КСЗІ, яке містить основні технічні вимоги до КСЗІ, а також узгоджені взаємні зобов'язання замовника і

виконавця розробки. Технічні вимоги визначають значення основних технічних характеристик, виконуючі функції, режими роботи, взаємодію із зовнішніми системами і т. д. *Апаратні засоби* оцінюються наступними характеристиками: швидкодія, продуктивність, ємність запам'ятовуючих пристроїв, розрядність, вартість, характеристики надійності та ін. *Програмні засоби* характеризуються потрібним обсягом оперативної і зовнішньої пам'яті, системою програмування, сумісністю з ОС та іншими програмними засобами, часом виконання і т. д.

Науково - дослідна розробка починається з аналізу загроз безпеки інформації, аналізу КС, якій створюємо захист та аналізу конфіденційності і важливості інформації в КС. Насамперед проводиться аналіз конфіденційності і важливості інформації, що повинна оброблятися, зберігатися і передаватися в КС. На основі аналізу робиться висновок про доцільність створення КСЗІ. Якщо інформація не є конфіденційною і легко може бути відновлена, то створювати КСЗІ немає необхідності. Немає сенсу також створювати КСЗІ в КС, якщо втрата цілісності та конфіденційності інформації пов'язана з незначними втратами (рисунок 1).

При аналізі інформації визначаються потоки конфіденційної інформації, елементи КС, в яких вона обробляється і зберігається. На цьому етапі розглядаються також питання розмежування доступу до інформації окремих користувачів і цілих сегментів КС. На основі аналізу інформації визначаються вимоги до її захищеності. Вимоги задаються шляхом присвоєння певного грифу конфіденційності, встановлення правил розмежування доступу.

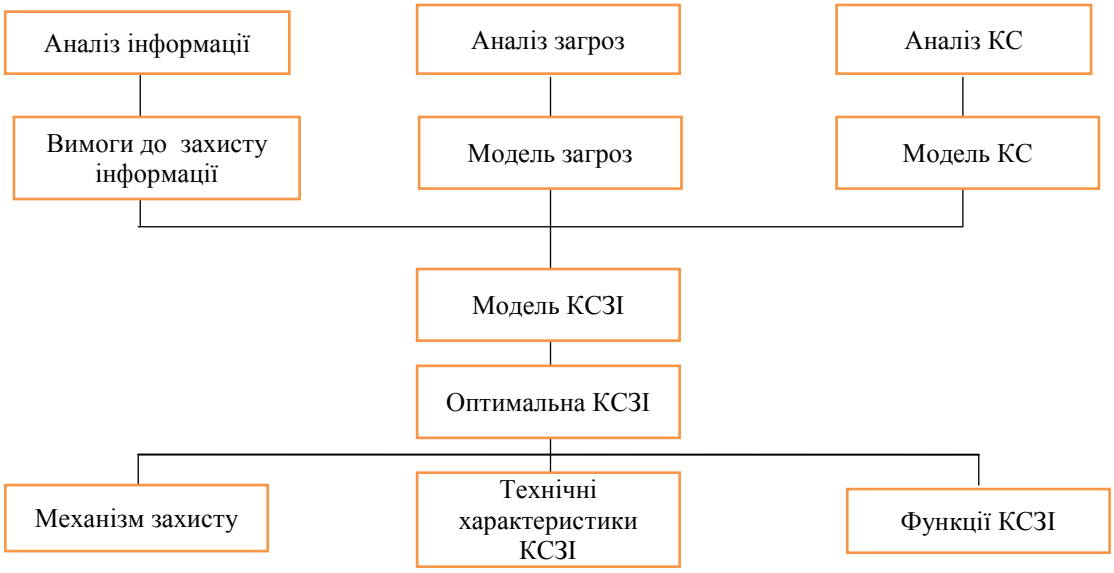

Рисунок 1 – Зміст науково-дослідницької розробки КСЗІ

Дуже важлива вихідна інформація для побудови КСЗІ виходить в результаті аналізу захищаємої КС. Так як КСЗІ є підсистемою КС, то взаємодію системи захисту з КС можна визначити як внутрішню, а взаємодію з зовнішнім середовищем - як зовнішню.

Внутрішні умови взаємодії визначаються архітектурою КС. При побудові КСЗІ враховуються:

- географічне положення КС;
- тип КС (розподілена або зосереджена);
- структури КС (технічна, програмна, інформаційна і т. д.);
- продуктивність і надійність елементів КС;
- типи використовуваних апаратних і програмних засобів і режими їх роботи;

• загрози безпеки інформації, які породжуються всередині КС (відмови апаратних і програмних засобів, алгоритмічні помилки і т. п.).

Зовнішні умови:

• взаємодія із зовнішніми системами;

• випадкові і навмисні загрози.

Етапи проектування систем захисту інформації

- проектне обстеження, яке формує базові вимоги до проектованої системи ЗІ;
- аналіз вимог, що пред'являються замовником до системи;
- проектування програмної та апаратної компонент - перетворення вимог в детальні специфікації системи;
- конструювання - виконання організаційно-технічних заходів, пов'язаних з розробкою і тестуванням компонент системи;
- верифікація спроектованої системи вимогам безпеки;
- реалізація і введення СЗІ в експлуатацію.

Принципи проектування систем захисту інформації

1. Принцип кінцевої мети означає, що будь-яка спроба зміни складу чи вдосконалення процедур застосування програмних і апаратних компонент захисту повинна оцінюватися з точки зору впливу на кінцеву мету, яка забезпечується інформаційно-керуючою системою і в якій проектована система є складовою частиною (підсистемою).

2. Принцип вимірювання передбачає необхідність кількісної оцінки характеристик СЗІ, які розкривають, насамперед, її цільові властивості.

3. Принцип еквівалентності (завершеності) передбачає забезпечення захисту інформації, засобів інформатизації, інтересів учасників інформаційних відносин і неможливість несанкціонованого доступу до інформації, що захищається при будь-яких станах зовнішнього середовища.

4. Принцип єдності означає, що при розробці елементів і підсистем необхідно орієнтуватися на досягнення інтегративного (системного) ефекту, тобто їх якісні та функціональні характеристики повинні підвищувати ефективність системи в цілому.

5. Принцип зв'язності означає, що для проектування та ефективного управління СЗІ в рамках організації необхідно розглядати СЗІ як підсистему її інформаційно-керуючої системи. Безліч функцій СЗІ при цьому буде знаходитися в залежності від зв'язків організації із зовнішнім середовищем, тобто з ієрархічними системами, а також внутрішніми зв'язками між структурними підсистемами.

6. Принцип модульної побудови дозволяє значною мірою абстрагуватися від надлишкових деталей, розглядаючи підсистеми СЗІ у вигляді «чорних ящиків», тобто акцентуючи увагу на їх входах і виходах. При цьому використання типових алгоритмічних і програмних рішень, засобів автоматизації та зв'язку, інших технічних елементів дозволяє знизити вартість і підвищити ефективність СЗІ.

7. Принцип ієрархії передбачає поетапні розробку і введення різних рівнів СЗІ (організаційно-управлінські, технічні і т.д.). Це видається особливо корисним при розробці складних СЗІ.

8. Принцип функціональності означає, що якщо існуюча технічна, технологічна, управлінська, кадрова і т.д. структура системи не дозволяє забезпечити необхідні функціональні можливості, то така структура повинна бути змінена (перепроектована).

9. Принцип розвитку забезпечує можливості модернізації та розширення функціональних можливостей СЗІ.

10. Принцип розумного поєднання централізації і децентралізації вимагає раціонального поєднання елементів централізованого та децентралізованого управління СЗІ. Для управління технічними системами централізація підвищує керування, але знижує надійність.

11. Принцип невизначеності, найчастіше пов'язаний з «людським фактором». Необхідно звести до мінімуму можливий збиток від неправильних дій персоналу і робити це слід ще на стадії проектування.

Список літератури

1. Гладких А.А. Базові принципи інформаційної безпеки обчислювальних мереж / А.А.Гладких, В.Є. Дементьєв. - Ульянівськ: УлГТУ, 2009. – 156 с.

2. Завгородний В.И. Комплексная защитаинформации в компьютерных системах / Учебное пособие.- М.:Логос; ПБОЮЛН. А.Егоров, 2001. - 264с.

3. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер - СПб.:Питер, 2003.—368с.:ил.— (Серия «Классик a computer science»).

УДК 004.738.5:004.056

Комплексні системи захисту для виявлення мережевих атак

Циганенко О.М., спеціаліст І категорії, інженер із застосування комп'ютерів
Кіровоградський національний технічний університет, м. Кіровоград

Захист інформаційної системи дає найкращі результати, якщо до неї підходити комплексно. Комплексна система захисту включає в себе захист об'єктів інформаційної системи, захист каналів зв'язку, процесів, програм і процедур обробки інформації, управління системою захисту, захист інформаційних мереж. В даний час захист інформації є важливою частиною інформаційних систем і в останні роки розвивається дуже добре. Воно й зрозуміло, адже чим далі, тим більше ми приходимо до розуміння, що найцінніший ресурс - це інформація, і вона теж потребує захисту. Головний напрямок пошуку нових шляхів захисту інформації полягає не просто у створенні відповідних механізмів, а являє собою реалізацію регулярного процесу, здійснюваного на всіх етапах життєвого циклу систем обробки інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи і заходи, використовувані для захисту інформації, найбільш раціональним чином об'єднуються в єдиний цілісний механізм – причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також нештатних ситуацій технічного характеру.

Для мінімізації ризиків інформаційної безпеки в інформаційних мережах в наш час актуальним є комплексний підхід для виявлення мережевих атак. Цей підхід включає в себе розробку та впровадження систем виявлення мережевих атак. Вони представляють собою спеціалізовані програмні або програмно-апаратні засоби, які дозволяють здійснювати активний аудит та управління безпекою (прогнозувати, виявляти, попереджувати, контролювати, реагувати в реальному масштабі часу на ризики безпеки) в мережі. Розв'язання задач для здійснення ефективного захисту інформації від мережевих атак вимагає розробки нових методів, які спроможні протидіяти розподіленим мережевим атакам різного походження та більш адекватно відображати складну динаміку випадкових процесів цих атак. Потрібна розробка методів виявлення розподілених мережевих атак, які використовують комплексні сучасні методи підтримки прийняття рішень на основі теорії інтелектуальних систем, що дозволяють здійснювати перехід від процесів виявлення і ліквідації до процесів прогнозування та попередження в реальному масштабі часу.

Розрізняють декілька методів виявлення мережевих атак:

- виявлення атак зловмисної поведінки;
- виявлення атак аномальної активності;
- багатоагентні системи виявлення аномальної мережевої активності.

Технологія виявлення атак зловмисної поведінки базується на виявленні атаки, яка потребує розуміння очікуваної поведінки порушника інформації, який підлягає контролю. Робота систем виявлення зловживань ґрунтується на складанні шаблонів. Захисні системи цього типу мають ефективність на відомих схемах атак, однак у випадку нової невідомої атаки або відхилення від шаблону, виникають проблеми. При цьому необхідно постійно підтримувати та оновлювати велику базу даних, яка включає не тільки атаки та її варіації, та безперервно поповнювати бази шаблонів. Крім цього важливо правильно визначати об'єм вибірки параметрів, які контролюються методом виявлення мережевої атаки, яка базується на зловмисній поведінці.

Технологія виявлення мережевих атак, яка базується на методах виявлення аномальної активності, відрізняється від розглянутої вище. Вона більш гнучка та дозволяє виявляти невідомі атаки. Системи виявлення аномалій ґрунтуються на припущенні, що всі дії зловмисника обов'язково відрізняються від поведінки звичайного користувача, тобто його дії вважаються аномальними. Виявлення атак обумовленні аномальною активністю та основані на порівнянні поточних значень параметрів активності , значення яких на даний момент визнані нормальними. Дана технологія базується на тому, що аномальна поведінка суб'єкта (системи, програми, користувача), проявляється як відхилення від нормальної поведінки. Ця технологія вимагає постійної реєстрації всіх дій об'єкту, що контролюється, яка необхідна для виявлення аномальної активності.

Враховуючи перспективи розвитку систем інформаційних технологій, а також об'єктивні недоліки, описаних попередньо двох комплексних підходів виявлення мережевих атак, можна зробити висновок про необхідність розробки та впровадження комплексних методів побудови систем захисту, які базуються на розподілених обчислювальних системах та з використанням механізмів захисту на основі активного аудиту.

Складові компоненти таких систем повинні бути спеціалізовані по типам задач, що необхідно розв'язувати, взаємодіяти один з одним з метою обміну інформацією та прийняття злагоджених рішень, адаптуватися до реконфігурації апаратного та програмного забезпечення мережі, зміни трафіку, новим видам атак та їх варіацій. Серед можливих технологій реалізації такого комплексного підходу, який є найбільш перспективним, вважається технологія інтелектуальних багатоагентних систем. Дана технологія полягає в наступному: компоненти системи захисту інформації (агенти захисту) являють собою інтелектуальні автономні програми, які реалізовують визначені функції захисту з метою забезпечення необхідного класу захисту. Вони дозволяють реалізувати комплексну надбудову над механізмами безпеки мережевих програмних засобів, операційних систем та додатків, які використовуються, при цьому підвищуючи захист системи до необхідного рівня. Виконання процесу прогнозування та виявлення розподілених мережевих атак – є ключовим фактором специфічних функцій багатоагентної системи виявлення мережевих атак.

Виявлення мережевих атак на ресурси систем інформаційних технологій – дуже складний технологічний процес, який пов'язаний зі збором великої кількості інформації про функціонування систем інформаційних технологій, аналізом цього об'єму даних та виявлення факту атаки. Для ефективного прогнозування та виявлення атак необхідне комплексне застосування різних методів виявлення мережевих атак. Оскільки вирішення проблеми підвищення ефективності захисту інформації в мережах залежить від використання адаптивних методів, це дозволить в реальному часі виявляти нестаціонарні

процеси, характерні для мережевих атак, та вчасно застосовувати комплексний підхід для вирішення даної проблеми. Цей підхід об'єднує в собі метод багатоагентних систем та метод адекватного виявлення ознак атак на основі статистичних методів теорії ймовірностей, нечітких статистичних методів, методів теорії інтелектуальних систем та методів штучних нейронних мереж.

При злагодженій реалізації даних методів в системі виявлення мережевих атак, можна досягти в широкому діапазоні умов функціонування мереж.

Список літератури

1. Земцов Ю.В. Комплексный подход к обнаружению сетевых атак [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/doc/zemcov.doc

2. Биячуев Т.А. Безопасность корпоративных сетей /под ред. Л.Г. Осовецкого., СПб ГУ ИТМО, 2004 – 161с.

3. Климов С.М., Сычёв М.П., Астрахов А.В. Противодействие компьютерным атакам. Методические основы : Электронное учебное издание

4. Девянин П.Н. Модели безопасности компьютерных систем: Учебн. Пос. для студ. ВУЗ / П.Н.Девянин – М.: изд. Центр «Академия», 2005.- 144с.

5. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебн. Пос.– М.: Логос; ПБОЮЛ Егоров Н.А., 2001. - 264с., ил.

Напрямок 8.
Захист персональних даних

УДК 004.056.5 (043.2)

Захист персональних даних в інформаційних системах

Бойко І.В., студентка 4 курсу
Науковий керівник – Казмірчук С.В., канд. техн. наук, доцент
Національний авіаційний університет, м. Київ

Україна робить свої перші кроки на шляху до формування високих стандартів захисту персональних даних (ПД). При виборі надійного ділового партнера серед українських організацій, іноземні компанії нерідко перевіряють ступінь захисту особистої інформації. Актуальність захисту ПД в Україні зумовлена не тільки розвитком автоматизованих систем обробки та зберігання інформації, але й формуванням баз даних у фінансовій, адміністративній, правоохоронній, медичній, маркетинговій сферах та використанням інформаційних технологій кримінальними структурами. Тому необхідно створити таку систему захисту персональних даних (СЗПД), що забезпечила б прозорість і довірчі відносини між Україною та її міжнародними партнерами. Аналіз останніх досліджень показав, що загрози інформаційній безпеці за своєю значимістю посідають друге місце серед основних загроз бізнесу, таких як економічна нестабільність, промислове шпигунство, викрадення інтелектуальної власності, нанесення шкоди репутації, тощо. Встановлено, що питання внутрішньої безпеки інформаційних систем (ІС), зокрема і питання неконтрольованого поширення даних, на поточний час є актуальними. Це викликано стабільно зростаючою кількістю зафіксованих випадків витоку інформації у всіх країнах світу. При цьому 70-90% даних, що втрачаються, складають ПД, третина з яких втрачається мережевим шляхом. Приблизно однакові частки втрати ПД спостерігаються як за рахунок навмисних дій співробітників компаній, так і через їх необережність. Невирішеними залишаються завдання створення єдиної методології проектування СЗПД, яка б дозволяла комплексно вирішувати проектні процедури, здійснювало обстеження ІС, використовувала б як вітчизняні [1] так і міжнародні нормативи щодо захисту ПД, і за необхідності могла б бути сумісна або інтегрована до вже існуючих ІС. Тому, метою даної роботи є формування вимог щодо забезпечення СЗПД. При цьому потрібно вирішити наступні завдання: проаналізувати загальні та створити додаткові принципи обробки ПД та розробити загальні рекомендації щодо їх захисту.

При створенні, функціонуванні та розвитку національної інформаційно-комунікаційної інфраструктури особливе місце займають вимоги щодо захисту ПД, запобігання несанкціонованому поширенню, використанню, порушенню цілісності, конфіденційності, доступності інформації і тим самим запобігання нанесення шкоди життєво важливим інтересам людини, суспільства і держави. Особливістю інформації, яка циркулює в ІС обробки персональних даних (ІСОПД), є її конфіденційність. У відповідності до Закону України «Про захист персональних даних» оператори, які обробляють ПД, зобов’язані

вживати необхідних та достатніх заходів щодо обмеження несанкціонованого доступу до ПД, збереження їх цілісності та попередження неконтрольованого поширення. Тому однією із основних вимог при роботі ІСОПД є забезпечення та підтримка визначеного рівня інформаційної безпеки їх ресурсів. Рівень безпеки таких систем, визначається ступенем захисту інформації від несанкціонованого доступу до неї, а також захищеністю від втрати та спотворення даних, що обробляються. При цьому забезпечення необхідного рівня безпеки ІСОПД включає комплекс організаційно-технічних заходів, які виключать або суттєво мінімізують можливість несанкціонованого поширення інформації, спотворення або знищення даних [2].

В доповнення до принципів, встановлених чинним законодавством України, необхідно аналізувати існуючі та впроваджувати нові принципи обробки ПД, таких як: організації повинні поважати конфіденційність ПД, які обробляють у своїй професійній діяльності; повинні збалансовувати потреби суб'єктів відносин, пов'язаних із ПД. Організації повинні запевняти, що їх професійна діяльність, пов'язана з обробкою ПД, виконується особами з відповідними навичками, досвідом та усвідомленням принципів закону та моральних норм. Також, повинні відслідковувати будь-які зміни в законодавстві щодо захисту ПД, а також передового досвіду у сфері їх захисту. Загальні рекомендації щодо захисту ПД повинні включати: послуги, які надає організація, повинні надаватися у відповідності з чинним законодавством України або законами інших юрисдикцій, які пов'язані з проектом, якщо це необхідно; організації повинні брати на себе відповідальність за всі необхідні заходи щодо захисту ПД, щоб уникнути конфлікту інтересів з клієнтами та/або суб'єктами ПД; необхідно враховувати, що організації повинні здійснювати свою діяльність з усвідомленням постійної загрози електронних атак злочинців, які діють в кіберпросторі, та можуть призвести до порушення захисту ПД; відповідно, вони повинні бути готовими відреагувати на будь-яке порушення безпеки швидко та ефективно; організації повинні розробляти та організовувати відповідні рівні безпеки; безпосередні виконавці можуть отримати доступ і обробляти ПД тільки в межах своїх повноважень; організації повинні брати на себе відповідальність за всі необхідні заходи для забезпечення того, що якщо ПД були випадково втрачені, змінені або знищені, вони можуть бути відновленими; організації, які є володільцями даних, повинні дотримуватися вимоги щодо реєстрації баз ПД в Державному реєстрі баз ПД.

Було розглянуто основні вимоги щодо СЗПД, що для забезпечення необхідного рівня безпеки має бути комплекс організаційно-технічних заходів. Проаналізовані та створені додаткові принципи, які доповнюють законодавство, і тим самим розширюють поле обробки ПД. Також, були розроблені загальні рекомендації до їх захисту, що підкреслюють важливість забезпечення захисту ПД.

Список літератури:

1. Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI (Редакція станом на 09.06.2013).

2. Філоненко С.Ф. Захист інформації в системах обробки персональних даних / С.Ф. Філоненко, В.А. Швець, І.М. Мужик // Захист інформації, Том 15. – 2013. - №4. – С. 307-315.

УДК 004.056.5

Базові параметри представлення ризику захисту персональних даних в державних АС

Дрейс Ю.О., канд. техн. наук, доцент
Житомирський військовий інститут імені С.П. Корольова, м. Житомир

Важливою складовою державних інформаційних ресурсів є персональні дані (ПД). Сьогодні забезпечення захисту ПД потребує неабиякої уваги, про що наголошується у рішенні Ради національної безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 [1]. А саме про необхідність вживання додаткових заходів щодо захисту інформації з обмеженим доступом (насамперед ПД, що належать до конфіденційної інформації) під час її обробки в автоматизованих системах (АС). Згідно з вимогами Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [1] для забезпечення безпеки державних інформаційних ресурсів, оброблюваних в автоматизованій системі, необхідно розробляти комплексну систему захисту інформації (КСЗІ).

Аналіз і оцінка ризику

Для побудови КСЗІ та інших систем безпеки необхідно проводити аналіз і оцінку ризиків (далі – АОР). *Аналіз ризику* – процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеню їх прийнятності для експлуатації АС. *Оцінка ризику* – дослідження об'єкта оцінки з метою визначення можливості реалізації загроз. Існуючі засоби АОР в переважній своїй більшості засновані на статистичних підходах. У багатьох країнах, як на рівні підприємств, так і на державному рівні подібна статистика не ведеться. Це обмежує можливості існуючих засобів АОР, наприклад, щодо використання різних типів вхідних даних для оцінки. Для визначення типів вхідних, внутрішніх та вихідних параметрів (як базових параметрів представлення ризику), які використовуються для АОР захисту ПД досліджено норми Закону України «Про захист персональних даних» [3], «Типовий порядок обробки ПД в базах ПД АС» [4], існуючі стандарти і методики оцінювання ІТ-ризиків.

Базові параметри ризику захисту ПД

Інтегроване представлення параметрів ризику з відображенням на сферу захисту ПД здійснюється у вигляді конкретного кортежу. Кортеж параметрів ризику захисту ПД можна представити у наступному вигляді [5]: $< A, B, C, D, E, F, G, H, I >$, де A – характеристика ПД (ідентифікація їх складу та змісту); B – характеристика середовища обробки БПД в АС; C – мета обробки ПД; D – аудит застосованих механізмів безпеки; E – характеристика існуючих функціональних послуг; F – ідентифікація загроз захисту ПД при обробці БПД в АС; G – величина можливого збитку від витоку ПД (чи БПД в АС); H – ОР захисту ПД; I – керування ризиком та досягнення необхідного рівня гарантій захисту ПД.

Список літератури

1. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки [...] / РНБО; Рішення від 28.04.2014 {введення в дію від 01.05.2014}.

2. Про захист інформації в інформаційно-телекомунікаційних системах / Верховна Рада України; Закон від 05.07.1994 № 80/94-ВР {редакція від 19.04.2014}.

3. Про захист персональних даних / Верховна Рада України; Закон від 01.06.2010 № 2297-VI {редакція від 30.05.2014}.

4. Про затвердження документів у сфері захисту персональних даних / Уповноважений ВР з прав людини; Наказ, Порядок, Форма типового документа [...] від 08.01.2014 № 1/02-14.

5. Підхід до аналізу і оцінки ризиків захисту персональних даних в державних автоматизованих системах / Ю.О. Дрейс, А.О. Дейсан, Д.Ю. Бєляк / 68-ма наук.-техн. конф. професорсько-викладацького складу, науковців, аспір. та студ.: Матеріали конф., 4-6.12.2013 р., Част.3. – Одеса.: ОНАЗ ім. О.С. Попова, 2013. – С.117-120.

УДК 004.056.5

Огляд загроз безпеки інформації в соціальних мережах

Константинова Л.В., викладач
Кіровоградський національний технічний університет, м. Кіровоград

В теперішній час соціальні мережі набули великої популярності. Практично кожен Інтернет-користувач є власником особистої сторінки, а може і не єдиної. Соціальні мережі активно використовуються не тільки для особистого спілкування, але і для вирішення ділових задач, що має на увазі застосування інформації - одного з найбільш цінних продуктів людської діяльності. Часто створюються умови для реалізації загроз безпеки інформації [1]. Для того щоб убезпечити себе від шахраїв та інших злочинників в соціальних мережах важливо мати уявлення про методи соціального зламу а також застосовувати методи захисту від нього.

Можна сказати, що стосовно до Інтернету поняття соціальна мережа - це віртуальна мережа, яка є засобом забезпечення сервісів, пов'язаних із встановленням зв'язків між його користувачами, а також різними користувачами та відповідними їх інтересам інформаційними ресурсами, встановленими на сайтах глобальної мережі [2].

Згідно класичного визначення Д. Бойд, соціальні Інтернет-мережі – це мережеві послуги, які дозволяють приватним особам створювати соціальні та напівсоціальні профілі у рамках обмежень, які накладаються системою, визначати список інших користувачів, з якими вони можуть ділитися інформацією, оглядати та зв'язувати їх список контактів з іншими, створеними користувачами всередині системи [3].

Оглянемо декілька загальних рис, якими володіють всі сучасні системи забезпечення роботи мережевих спільнот:

- в більшості співтовариств передбачається реєстрація користувачів – тобто на кожного учасника повинен заводитись обліковий запис. Під час реєстрації користувач повинен вказати про себе деяку інформацію для ідентифікації. Відбувається перевірка адреси електронної пошти, на яку відсилається код активації облікового запису. Якщо адреса невірна, то активувати запис може тільки адміністратор системи. Цей метод гарантує в певній мірі унікальність учасника;
- кожен користувач вказуючи своє ім'я та підтверджуючи себе паролем починає сеанс роботи в середовищі. Зазвичай сеансовість роботи приховується від користувача технічними засобами, тим не менш, ідентифікація користувача відбувається постійно;
- користувач налаштовує оточення – зовнішній вигляд, додаткову інформацію про себе (вказує особисті інтереси, місця відпочинку, дані про роботу) окрім облікових даних;
- соціальні мережі та сервіси, що їх підтримують можна розглядати, як ефективний метод забезпечення відвідуваності сайтів, зворотного зв'язку, а також, можна відмітити, одним із засобів генерації контенту (вмісту, що має цінність) [2].

Виходячи з цих визначень, можна зробити висновок, що шахраїв можуть зацікавити персональні дані, які надаються користувачами.

Загрозою безпеки персональної інформації може бути злом пароля. Хакеру для цього не потрібно багато часу. Прості паролі можливо зламати без застосування спеціальних програм. Складні ж паролі зламуються за допомогою спеціальних програм-зломщиків. Ці програми вміщують словарі з паролями. Залишається тільки підібрати пароль [4]. Ця загроза несе за собою в першу чергу розсилку різного роду спаму. Крім того в цій ситуації є велика ймовірність злому всіх поштових скриньок, що були вказані у зламаному акаунті. Крім того

все це сприяє психологічним проблемам, крім неприємностей, можливо, прийдеться витрачати час на створення нового акаунту, створення нового пароля, зміну паролів на інших акаунтах і поштових скриньках.

Для запобігання таких ситуацій необхідно вибирати паролі, що відповідають деяким вимогам. Пароль повинен бути достатньо складним (містити цифри, малі літери та заголовні, знаки). Довжина паролю повинна бути більше восьми, а краще десяти символів.

Інший метод отримати доступ до акаунту користувача соціальних мереж здійснюється через викрадення cookies [4]. Cookies це – невеличкий фрагмент службової інформації, який веб-сервер розміщує на комп'ютері користувача та застосовується для зберігання даних, специфічних для користувача та використовується веб-сервером для різних цілей. Ці файли можуть зберігати будь-які користувацькі налаштування (ключ сесії, зашифрований пароль, комбінацію з зашифрованого пароля і логіна). Зловмисники це роблять маючи доступ до користувацького комп'ютера або через Інтернет-з'єднання, що називається зламом сесії.

Захист cookies надають захищені канали (HTTPS-сесія плюс атрибут «SECURE» в самих cookies). Простіше всього стати жертвою таким чином у місцях найменш захищених та найбільш масових (наприклад, кав'ярня з доступом до wi-fi).

Наступний метод доступу до конфіденційної інформації користувачів, що використовується Інтернет-шахраями, називають фішинг [4]. В перекладі з англійської мови фішинг (phishing) від fishing – вивуджування. Зловмисники зазвичай у якості приманки в соцмережах використовують лист або особисте повідомлення від адміністрації якогось популярного сервісу (банку, комп'ютерної компанії або подібної соціальної мережі та ін.), в якому пропонують, наприклад, проголосувати за фотографію або внести плату за послуги. Необачні користувачі за посиланням потрапляють на фішинговий сайт. Шахраї отримують персональні дані користувача, навіть якщо він щось встиг запідозрити та швидко покинути сайт. Також цим методом можливо розповсюджувати зловмисний код та проводити розвідку, щоб потім здійснювати направлену атаку [6].

Для захисту від фішингу необхідно відправляти листи від підозрілих незнайомих користувачів в папку «Спам» та інформувати адміністрацію, а також не потрібно розголошувати паролі від акаунтів.

Програми для викрадення паролів [4] – це ще один тип загроз інформаційній безпеці, який мігрував з систем Інтернет-банкінгу. Вони викрадають реєстраційні дані користувача соцмережі, ще до того, як ті відправляються на сервер, завдяки впровадженню частини свого коду в браузер. Дані викрадаються всередині браузера і тому шифрування SSL-з'єднання між комп'ютером користувача і веб-сайтом не може захистити. Якщо шахраї отримують інформацію користувача, то можна очікувати встановлення посилок для крадіжки паролів на комп'ютери друзів.

Програми для викрадення паролів вважають шкідливим ПЗ, яке встановлюється локально на комп'ютер, і тому кращий метод захисту від них – сучасні антивірусні засоби.

Фармінг – ще один вид загроз інформаційній безпеці, що з'явився в процесі еволюції фішингу та є більш небезпечнішим. Зловмисники перенаправляють користувача-жертву на хибну IP-адресу, але навіть дуже уважний користувач не може відрізнити фармінг-сайт від потрібного, якщо у нього немає можливості оглядати IP-адреси сайтів та порівнювати їх.

Троянські програми, фальшиві антивіруси, соціальні черв'яки, які застосовують для власного розповсюдження списки друзів, та ін. [6] – все це засоби, які використовують хакери для того, щоб організовувати атаки на вразливості у браузерах через соціальні мережі також. Їх основна мета проникнути та закріпитись в інформаційній системі відвідувача соцмережі.

Велику загрозу інформаційної безпеки в соціальних мережах несуть соціальні хакери [7]. Це люди, які володіють здібностями та знаннями, щоб «зламати людину», запрограмувавши її на вигідні йому дії. Соціальні хакери застосовують методи соціальної інженерії такі, як трансактивний аналіз, нейролінгвістичне програмування для різних зловмисних цілей. Вони створюють такі ситуації, коли користувачі самі надають

зловмисникам відомості. Це може бути або некомфортний психологічний стан людини, що змушує людину прийняти швидке і невірне рішення, або може бути, навпаки, створення довірчої атмосфери [5]. Можна зустріти в соцмережах загрозу під назвою «маскарад», тобто можливість підміни особистості: достеменно невідомо, хто ховається під іменем друга. Результатом шахрайського сценарію може бути «чорний піар» або «антипіар».

Через соціальні мережі можуть взаємодіяти екстремісти. За допомогою соцмереж «модерувались» конфлікти в Єгипті і Сирії, заворушення в Лондоні [6]. Контроль над діями, що відбуваються в соцмережах повинен проходити на рівні держави. Це питання є особливо важливим для України в ці часи. Тому міністерство оборони закликає пересічних українців з обережністю відноситись до інформації, яка публікується в мережах, оскільки деякі дані можуть використовуватись для підриву морального духу громадян України та перевіряти інформацію, звертаючись до офіційних джерел [8].

Щоб захистити свою сторінку та персональні дані необхідно застосовувати механізми безпеки, які надаються соцмережами, загальні механізми безпеки, які не пов’язані з соцмережами, також перебуваючи в соціальній мережі не потрібно виконувати дії, які можуть погрожувати безпеці даних [5]. Тобто уважно відноситись до налаштувань доступу до своїх даних інших користувачів. До загальних механізмів безпеки, які не пов’язані з соцмережею можна віднести застосування захищеного протоколу взаємодії з Web-серверами (https), що гарантує безпечну передачу інформації мережею. Необхідно слідкувати та час від часу очищати дані з комп’ютера а також телефона, що стосуються профілю користувача соціальної мережі, які залишаються браузером у вигляді файлів та записів. Важливим також є використання антивірусів та фаєрволів. А також важливим є пильність та обачність самого користувача у відносинах з іншими користувачами.

Соціальні мережі зараз доволі широко поширені. Завдяки ним можливо тримати зв’язок навіть з людьми, що від нас на відстані, отримувати як великий спектр можливостей так і велику кількість загроз інформаційній безпеці.

Прості користувачі, підприємства (або фірми), держави будують свою життєдіяльність на основі достовірних відомостей, збереження яких фактично є головним фактором їх функціонування. Виходячи з усього вище сказаного, вкрай важливим зараз є обізнаність у сфері інформаційної безпеки. Крім того методи негативного впливу на інформацію і на особистість постійно удосконалюються, а це означає, що життєво необхідно вдосконалювати механізми захисту інформації і не тільки у соціальних мережах.

Список літератури

1. Хорев А.А., Угрозы безопасности информации, Московский государственный институт электронной техники (технический университет), г.Москва, журнал "Специальная Техника" №1 2010 год [Інтернет ресурс] – Режим доступа: http://www.bnti.ru/showart.asp?aid=955&lvl=04.03.

2. Ефимов Е.Г. Кузнецов А.А. Виды кризисного потенциала социальных сетей как региональных социально-экономических систем // Инновационный потенциал современного региона: проблемы региональной безопасности и внутрирегиональной интеграции на постсоветском пространстве, всерос. научн.-практ.конф. Всероссийская научно-практическая конференция «Инновационный потенциал современного региона: проблемы региональной безопасности и внутрирегиональной интеграции на постсоветском пространстве», 28-29 октября 2011 г., – Волгоград: Изд-во ФГОУ ВПО ВАГС, 2011. – С.144-145.

3. Угрозы безопасности информации в социальных сетях Ивановский О.В. (Московский государственный технологический университет «СТАНКИН», Россия) ВС/NW 2011; №2 (19):11.4 [Інтернет ресурс] – Режим доступа: http://network-journal.mpei.ac.ru

4. Руслан Мамедов Защита персональных данных в социальных сетях. Журнал "Information Security" [Інтернет ресурс] – Режим доступа: http://www.itsec.ru/articles2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah

5. Олег Седов Угрозы социальных сетей. Настольный журнал IT-руководителя «Директор информационной службы» №12, 2011 [Інтернет ресурс] – Режим доступа: http://www.osp.ru/cio/2011/12/13012286/

6. Симдянов И., Кузнецов М. Социальная инженерия и социальные хакеры – СПб.:БХВ – Петербург, 2007-368с.:ил.

7. Вадим Ковальов Інформаційний бруд, як постріл у спину [Інтернет ресурс] – Режим доступа: http://narodka.com.ua/10634-informacijnij-brud-yak-postril-u-spinu

УДК 004.056.5

Безпека інформації у соціальних мережах

Притула С.В., студент 2 курсу
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Вступ

В наш час все більшої й більшої популярності набувають соціальні мережі. Найбільш популярними є такі соціальні мережі як : Facebook, Vkontakte, Google+, Twitter та ін. Все частіше ми чуємо про те що, соціальні мережі піддаються стороннім атакам та користувачі втрачають свою інформацію. Саме через це є необхідність проаналізувати, на якому рівні в наш час є безпека інформації в соціальних мережах та як користувачу зберегти свою інформацію.

Основна частина

Соціальні мережі - це відмінний спосіб бути на зв'язку з людьми, а мала дещиця здорового глузду щодо відомостей, наданих іншим людям, може послужити вам хорошу службу в збереженні безпеки та конфіденційності важливої інформації. Багато проблем безпеки особистості в сучасному інформаційному суспільстві вирішуються технічними методами. Але наприклад, спам, є абсолютно не технічною проблемою - техніка як раз успішно справляється з його передачею. Спам виник природним чином при розвитку економіки і рекламних технологій. У російському та українському сегменті Інтернету спам досягає 80% всього поштового трафіку - як видно проблема за десять з гаком років технічними фахівцями вирішена не була.

Більшість сайтів соціальних мереж використовують мережевий протокол HTTPS для безпечного з'єднання. HTTPS забезпечує шифрування даних при передачі по комп'ютерних мережах. Деякі сайти, такі як Twitter, Google+ використовують цей протокол за замовчуванням, на інших потрібно конфігурувати з'єднання HTTPS. Це гарантує безпечну передачу інформації по мережі, у тому числі зв'язки логін-пароль (але при цьому знижується швидкість передачі даних). Але дана технологія захисту повинна підтримуватися інформаційною системою (практично всі соцмережі її підтримують). Необхідно стежити і регулярно очищати дані про профіль користувача соціальної мережі, що залишаються браузером у вигляді файлів або записів на комп'ютері. У деяких випадках такі дані можуть використовуватися шкідливим ПЗ для отримання з них деяких важливих відомостей (наприклад, тієї ж зв'язки логін-пароль). У число рекомендацій іншого типу выдноситься встановлення на комп'ютер антивірусів та інших засобів захисту. Але не варто також забувати про мобільні пристрої, з яких останнім часом багато користувачів заходять у соціальні мережі. Дані пристрої локально зберігають персональні дані, отримані з соціальних мереж, і також схильні до дії шкідливого ПЗ. Таким чином, треба захищати і мобільні пристрої.

Поради, які допоможуть захистити приватну інформацію в соціальних мережах:

1. Перш за все для того щоб захистити свою інформацію у соціальній мережі найкращим захистом буде обмеження доступу до опублікованої інформації.

2. Необхідно ретельно продумувати, що публікувати в профілі, на форумах, в миттєвих повідомленнях або в будь-яких інших засобах спілкування, щоб не допустити крадіжку особистих даних або іншу шкідливу діяльність щодо себе. Такі відомості, як особисті і робочі імена, адреси, номери телефонів, дати народження і т.д. потенційно небезпечні, тому що можуть стати загальнодоступними. Необхідно використовувати в повідомленнях загальні формулювання, щоб зловмисник не зміг скористатися цією

інформацією.

3. Необхідно використовувати для захисту аккаунта тільки надійний пароль і нікому його не повідомляти або не використовути повторно для інших сайтів. Крім того, багато сайтів підтримують надійнішу автентифікацію, наприклад двоступеневу перевірку. По можливості, треба нею користуватися.

4. Під грифом секретності повинна залишитися і інформація про організацію користувача. Так, компанія Sophos, яка займається питаннями інформаційної безпеки, провела дослідження і з'ясувала, що близько 63% організацій побоюються зайвої балакучості своїх співробітників, які не задумуючись про наслідки можуть опублікувати цінну інформацію. Одним з найяскравіших прикладів подібного випадку є історія з компанією Microsoft. Через профілі співробітників "комп'ютерного гіганта" в соціальній мережі Linkedin журналістам неодноразово вдавалося отримати дані про будь-які новинки або плани компанії за кілька місяців до їх офіційного оприлюднення.

5. Треба бути обережним з підозрілими посиланнями або помилковими публікаціями на сайтах соціальних мереж. Кіберзлочинці можуть розміщувати шкідливі посилання. Якщо натиснути на них, то можна потрапити на шкідливі сайти, які спробують заразити комп'ютер.

6. Деякі соціальні мережі надають можливість встановити програми, створені сторонніми розробниками, наприклад, ігри. Ці програми піддаються мінімальній перевірці або зовсім не перевіряються на предмет наявності недекларованих функцій і небезпечного коду. Через них можна отримати контроль над аккаунтом або доступ до персональних даних. Необхідно встановлювати тільки ті програми, які дійсно потрібні, та завантажувати їх з відомих, перевірених сайтів і відразу ж видаляти після використання.

Висновки

Таким чином можна побачити, що безпека інформації у соціальних мережах це дуже вразливе місце. Хоча у самих соціальних мережах встановлюють засоби захисту інформації, це не може на усі 100% гарантувати, що вашу інформацію та персональні дані не зможуть викрасти та використати проти вас. Для збереження вашої інформації необхідно дотримуватись певних правил та стежити за інформацією, яка публікується на ваших особистих сторінках у соціальних мережах.

Список літератури:

1. Безопасность в социальных сетях [Електронний ресурс]. – Режим доступу: http://ru.norton.com/social-networking-safety/article

2. Безопасность личности в информационном обществе [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/post/109243/

3. Как обеспечить безопасность данных в социальных сетях [Електронний ресурс]. – http://www.microsoft.com/ru-ru/security/online-privacy/social-networking.aspx

Напрямок 9.
Інформаційні війни

УДК 004.056:32.019.51

Огляд методів інформаційно-психологічної війни

Артеменко А.С., студентка 4 курсу
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Інформаційні та психологічні війни тісно пов’язані з поняттям інформаційного простору. Під даним терміном розуміють не сукупність ЗМІ, які розташовані на визначеній території, а масову інформацію, яка породжується цими ЗМІ і яка сприймається населенням даної території. Це, свого роду, медіа-реальність.

Ціль інформаційної війни – досягнення інформаційного домінування. Задачею інформаційного домінування є не дати протилежній стороні скористатися інформаційним простором в повній мірі. [4]

Психологічна війна – це сукупність різних форм, методів і засобів впливу на людей з метою зміни в бажаному напрямі їх психологічних характеристик (поглядів, думок, ціннісних орієнтацій, мотивів, стереотипів поведінки тощо), а також групових норм, масових настроїв, суспільної свідомості в цілому. [3]

Психологічна війна використовує сегмент інформаційного простору для інформаційно-психологічного впливу на певну аудиторію. Інформаційні війни направлені на контроль над інформаційним простором в цілому.

В наш час багато держав розглядають психологічно-інформаційну війну як ефективний інструмент реалізації зовнішньої політики.

Інформаційно-комп'ютерна революція відкриває широкі можливості для впливу на народи та владу, маніпулювання свідомістю та поведінкою людей навіть на віддалених просторах. Беручи до уваги процес глобалізації телекомунікаційних мереж, що відбувається в світі, можливо припустити, що саме інформаційним видам агресії буде відданий пріоритет у майбутньому.

Науково-технічна революція, нові інформаційні технології, глобальні інтеграційні процеси спричинилися до формування глобального інформаційного співтовариства, у якому інформація стала головним чинником керування сучасним світом й основним інструментом влади.

Факт появи інформаційного простору призводить до появи бажаючих не лише поділити цей простір, а й контролювати і управляти процесами, що в ньому відбуваються. Для цього використовується так звана інформаційна зброя, яка являє собою засоби знищення, перекручення чи розкрадання інформації; засоби подолання систем захисту; засоби обмеження допуску законних користувачів; засоби дезорганізації роботи технічних засобів комп'ютерних систем.

Атакуючою інформаційною зброєю називають:

- комп'ютерні віруси;
- логічні бомби (програмні закладки);
- засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікація інформації у каналах державного та військового управління;
- засоби нейтралізації тестових програм;

- різного роду помилки, які свідомо вводяться в програмне забезпечення об'єкта. [2]

Засоби інформаційного впливу безпосередньо на людину, соціальні групи та соціум в цілому почали розроблятися в межах концепції "психологічних війн". [5]

Психологічна війна - це особливий вид війни, що дозволяє, використовуючи різні засоби (пропаганда, "промивання мізків", інформаційна обробка населення, підрив громадянського духу, деморалізація Збройних Сил, дезорієнтація командування і війна культур та інші) впливати на власні народи, народи ворожих, союзницьких і нейтральних країн у політико-ідеологічній, моральній і психологічній сферах для досягнення цілей своєї військової стратегії.

Метою психологічної війни є підготовка та ведення агресивних воєн в політико-ідеологічному, моральному і психологічному аспектах. Все це робиться насамперед для того, щоб вплинути на почуття людей, викликати панічний страх, порушити у народу ненависть до інших народів, зіграти на людських почуттях.

Поле дії психологічно-інформаційних воєн охоплює наступні області:

1) інфраструктуру систем життєзабезпечення держави - телекомунікації, транспортні мережі, електростанції, банківські системи тощо;

2) промислове шпигунство - розкрадання патентованої інформації, спотворення або знищення особливо важливих даних, послуг; збір інформації розвідувального характеру про конкурентів тощо;

3) злом і використання особистих паролів VIP-персон, ідентифікаційних номерів, банківських рахунків, даних конфіденційного плану, виробництво дезінформації;

4) електронне втручання в процеси командування і управління військовими об'єктами і системами, "штабна війна", виведення з ладу мереж військових комунікацій;

5) всесвітня комп'ютерна мережа Інтернет, в якій, за деякими оцінками, діють 150.000 військових комп'ютерів, і 95% військових ліній зв'язку проходять за відкритими телефонними лініями.

В основі психологічної війни лежать психологічні операції - планова пропагандистська і психологічна діяльність у мирний і воєнний час, яка розрахована на ворожі, нейтральні та дружні аудиторії з метою формування їх позитивного ставлення для досягнення як політичних, так і воєнних національних цілей держав.

Основні форми психологічних операцій [1]:

- пропагандистські дії - це систематизоване, цілеспрямоване розповсюдження ідей за допомогою різноманітних засобів зв'язку та інформації з метою впливу на думки, почуття, стани і ставлення або поведінку для досягнення прямої чи опосередненої користі для своєї країни;
- психологічні дії - це різні політичні, економічні та інші дії, які спрямовані на підрив позицій протилежної сторони та зміцнення власних позицій.

Задачі психологічних операцій [1]:

1. Переконання противника у правильності, необхідності військового втручання.
2. Вплив на військово-політичне керівництво противника і його союзників з метою їх відмови від війни.
3. Підтримка внутрішньої опозиції противника.
4. Підтримка та керування дисидентськими рухами.
5. Вплив на населення дружніх країн.
6. Сприяння розвитку позитивного відношення населення нейтральних держав.
7. Підрив морального духу противника.
8. Зниження боєздатності противника.
9. Аналітична робота щодо виявлення слабких місць противника та доведення цієї інформації до власних керівників.
10. Протидія інформаційному впливу противника тощо.

Основні методи психологічних операцій:

- метод розповсюдження наочних, звукових і відеозвукових пропагандистських матеріалів;

- методи здійснення практичних дій - інсценування повстанських дій, саботажу, демонстрація сили, масові мітинги тощо.

Під інформаційно-психологічною зброєю слід розуміти сукупність спеціальних засобів і технологій, що використовуються для насильницького спотворення інформаційно-психологічного простору супротивника для ураження індивідуальної і масової свідомості. Тобто, байдуже, що то є – технічні чи технологічні аспекти, головною мішенню інформаційно-психологічної війни стає людський розум.

Інформаційно-психологічна зброя (ІПЗ) може спрямовуватися на придушення, знищення, дезорганізацію, дезорієнтацію, дезінформацію, дезадаптацію об'єкта впливу; вона може порушувати психічне здоров'я, спонукати до спонтанних, немотивованих, агресивних дій, спричиняти тимчасові чи незворотні зміни в свідомості особистості, а то й самознищення її.

ІПЗ за формою впливу можна класифікувати умовно так [6]:

- Засоби радіоелектронної боротьби, тобто радіоелектронну розвідку, радіоелектронний захист та радіоелектронне придушення. Це пасивні і активні технічні засоби, що працюють в діапазоні електромагнітних хвиль від частки мікрометра до десятків тисяч кілометрів; радіоелектронні засоби інформаційного захисту і спостереження за різними об'єктами.

- Програмово-комп'ютерні технології. Це технічні засоби, алгоритми або технології, дія яких спрямовується на ураження комп'ютеризованих систем державного і військового управління супротивника, управління його енергосистемами, транспортом, загальною інфраструктурою життєзабезпечення через ініціалізацію та активацію в інформаційних системах спеціальних руйнівних програмових засобів (програмово-апаратних закладок, комп'ютерних вірусів, системних „хробаків", інших шкідливих і руйнівних програм), знищення об'єктів збирання, доставки, опрацювання, нагромадження й зберігання інформації, руйнування інформаційних масивів тощо.

- Психотронні засоби, які, через застосування відповідного випромінювання, порушують психічний чи психофізіологічний стан, впливають на сприйняття реальності, створюють неможливість адекватно реагувати на ситуацію.

- Психотропні засоби, які через застосування певних біологічних чи хімічних реагентів впливають на психосоматику, змінюють загальний психофізіологічний стан особистості, погіршують її самопочуття і розумові здібності, викликають депресію чи панічний страх, галюцинації тощо.

- Навіювання і гіпноз, НЛП (нейро-лінгвістичне програмування), інші техніки сугестивного впливу. Тут використовуються особливості людської психіки, завдяки яким особистість може піддаватися навіюванню і програмуванню. Передбачається директивність, тобто категоричність і обов'язковість виконання наказу (у випадку прямого навіювання) і неусвідомлене беззастережне виконання (під час гіпнотичного впливу).

- Символьно-семантичний апарат впливу, в тому числі віртуальний символізм

- Технології створення натовпу і управління ним.

- Загальна система обмеженого доступу до інформації. Передбачає примусове відчуження певної категорії інформації з міркувань державної і суспільної необхідності. Обмеження доступу встановлюється грифами на кшталт „державна таємниця", „особливо важливо", „цілком таємно", „таємно" тощо. Застосовується криптографія, тобто шифрування і дешифрування інформації.

- Технології заданого інформування і дезінформації. Сукупність маніпулятивних дій з інформацією для здобуття переваги над об'єктом впливу через дозоване цілеспрямоване інформування, ініціалізація навмисних витоків інформації, введення опонента в оману тощо. Дезінформація, як правило, подається в достовірному контексті, семантично різноплановому; має певну ешелонованість, тобто глибину наповнення, що підвищує її

вірогідність.

- Цензура. Це система нагляду за діяльністю видавництв і ЗМІ. Передбачає загальне управління інформаційним простором з боку суб'єкта, наділеного владним ресурсом.
- Пропагандистська діяльність. Націлюється на формування певного світосприйняття, морально-етичних норм, створення міфів та зразків наслідування через аудіо- і відеопродукцію, підручники, словники, енциклопедії тощо.
- Засоби масової інформації.

Підводячи підсумок, можна зробити висновок, що потрібно створити державну систему інформаційного протиборства, яка була б здатна акумулювати, координувати і направляти всі інформаційні дії, тим самим посилюючи процес інформаційного та культурного обміну.

Структура психологічно-інформаційної безпеки має відповідати таким сучасним викликам, як тероризм і політичний екстремізм, стояти на захисті індивідуума, суспільства, держави. Створення такої структури дозволить активно захищати наші національні інтереси в регіоні та у світі в цілому.

Список літератури

1. Ягупов В.В. Морально-психологічне забезпечення. – К:2002.
2. Расторгуев С.П. Информационная война. –М: Радио и связь,1999.
3. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, опыт). – Мн.: Харвест, 1999.
4. Поченцов Г.Г. Психологические войны. –М. - К.: Рефл-бук, Ваклер, 2000.
5. Требін М. Інформаційне суспільство. Війни нової епохи // Журнал «Вічне» 2002 № 4.
6 Лисенко В. Проблеми інформаційної незалежності держави – [Електронний ресурс] – режим доступу: http://www.politik.org.ua/vid/ magcontent.php3?m=1&n=59&c=1318&setcss=1&ncss=verybig

УДК 32.019.51:004.056.5

Дослідження методів ведення психологічних воєн

Білий В.С., студент 3 курсу
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Методи психологічного впливу у військових цілях відомі з давніх-давен. Фактично вони знайшли своє належне застосування з виникненням держави. Внаслідок накопичення досвіду практичного використання психологічного протиборства на війні, виникла необхідність в його теоретичному осмисленні та систематизуванні. Перші наукові обґрунтування психологічних воєн пов'язані з іменами давньокитайських філософів – Конфуція та Сунь-Цзи. Основні принципи ведення психологічних воєн докорінно не змінились, лише вдосконалились методи їх реалізації.

Психологічні протиборства отримали стрімкий розвиток на початку XX століття в ході Першої Світової Війни, коли стало зрозуміло, що фізичні форми впливу надзвичайно затратні. Військова перемога, отримана в такий спосіб, часто не окупає втрат живої сили та техніки. Виникла потреба в інтенсивному впровадженні інших засобів ведення війни – менш затратних, але подекуди й незрівнянно ефективніших. Сьогодні політики і фінансові кола, які стоять за ними не можуть прямо заявити, що війна ведеться заради захоплення джерел сировини і ринків збуту, заради знищення своїх економічних конкурентів, заради придушення визвольних рухів в колоніальних і напівколоніальних країнах, заради збереження влади транснаціональних корпорацій в країнах «третього світу», а аж ніяк не заради оборони або захисту свободи і демократії. Оскільки можновладці ніколи не можуть

сказати народам правду про справжні цілі війни, вони вдаються до психологічного насильства, брехні, пропагандистського цькування тих, хто не згоден стати гарматним м'ясом. Вдаватися до психологічної війни змушує те, що сучасні війни, які ведуть правлячі кола, суперечать інтересам народу

Психологічна війна – сукупність різних форм, методів і засобів впливу на людину з метою зміни в бажаному напрямку її поглядів, думок, цінностей, мотивів, а також групових норм, масових настроїв в цілому.

Існує чотири основні методи ведення психологічної війни: психологічні, військові, методи торгових та фінансових санкцій, а також політичні.

Водночас науковці виділяють шість основних типів психологічного впливу на людину:

1. Інформаційно-психологічний.

Психологічний вплив такого типу ставить своєю метою формування певних ідеологічних (соціальних) ідей, поглядів, уявлень, переконань, водночас воно викликає у людей позитивні чи негативні емоції, почуття, і навіть бурхливі масові реакції.

2. Психогенний.

Вплив такого типу є результатом:

а) фізичного впливу на мозок індивіду, в результаті якого спостерігаються порушення нормальної нервово-психічної діяльності.

б) шокового впливу оточуючих умов або якихось подій (картин масових руйнувань,численних жертв і т.п.) на свідомість людини, в результаті чого він не в змозі раціонально діяти, втрачає орієнтацію в просторі, відчуває афект, або депресію, впадає в паніку, ступор тощо.

3. Психоаналітичний – це вплив на підсвідомість людини терапевтичними засобами, особливо в стані гіпнозу чи глибокого сну. Існують також методи, що виключають свідомий опір як окремого індивіду, так і груп людей в стані бодрості.

4. Нейролінгвістичний.

Цей вплив також відомий під назвою «нейролінгвістичне програмування». Це різновид психологічного впливу, що змінює мотивацію людей шляхом введення в їх свідомість спеціальних лінгвістичних програм. Головним засобом впливу виступають спеціально підібрані вербальні і невербальні лінгвістичні програми, засвоювання вмісту яких дозволяє змінити в потрібному напрямку переконання, погляди і уявлення людини (як окремого представника, так і цілих груп).

5. Психотронний вплив – це вплив на інших людей, що здійснюється шляхом передачі інформації через позачуттєве сприйняття.

З урахуванням останніх досягнень не тільки в психології, але і "суміжних" науках (біології, нейро- і психофізіології, кібернетиці, психофармакології тощо) розробляються і продовжують удосконалюватися методи підпорогового впливу.

6. Психотропний – вплив на мозок і поведінку особистості шляхом введення в її організм різних препаратів (зокрема фармацевтичних препаратів, запахів), засвоєння яких відбивається на її вищій нервовій діяльності

Висновок. Результатом виконаної роботи є огляд та аналіз існуючих методів ведення психологічної війни. Було встановлено, що для різних ситуацій будуть ефективними різні способи. Наразі в світі розробляються шляхи одночасного поєднання всіх методів в політичних війнах.

Список літератури

1. Крысько В.Г. Секреты психологической войны / В.Г. Крысько – Мн.: Харвест, 1999. - 448 с.
2. Манойло А.В. Государственная информационная политика в особых условиях. / А.В. Манойло. – М.: МИФИ, 2003. – 388 с.

УДК 004.056.53

Інформаційна зброя та її застосування при веденні інформаційних війн

Гермак В.С., викладач
Кіровоградський національний технічний університет, м. Кіровоград

Сучасний рівень розвитку військового мистецтва відрізняється посиленням інформаційного протиборства. Це, перш за все, пояснюється такими властивостями інформаційної сфери, як невичерпність інформаційних ресурсів, можливість їх швидкого копіювання, переміщення практично без втрат на величезні відстані з високою швидкістю і мірою достовірності, компактність джерел і носіїв інформації, миттєва, але безкровна реакція (відгук) інформаційної сфери на дію, що важко ідентифікується відносно джерел.

Інформаційна зброя – це засоби знищення, спотворення або розкрадання інформаційних масивів, добування з них необхідної інформації після подолання систем захисту, обмеження або заборони доступу до них законних користувачів, дезорганізації роботи технічних засобів, виводу з ладу телекомунікаційних мереж, комп'ютерних систем, всього високотехнологічного забезпечення життя суспільства і функціонування держави.

Інформаційну зброю від звичайних засобів ураження відрізняє:

1) скритність - можливість досягати мети без видимої підготовки і оголошення війни;

2) масштабність - можливість завдавати непоправного збитку, не визнаючи національних меж і суверенітету, без обмеження простору у всіх сферах життєдіяльності людини;

3) універсальність - можливість багатоваріантного використання як військових, так і цивільних структур країни нападника проти військових і цивільних об'єктів країни, на яку здійснюється напад.

Якщо розглядати інформаційну зброю як сукупність засобів, що застосовуються для порушення (копіювання, спотворення або знищення) інформаційних ресурсів на стадіях їх створення, обробки, розповсюдження і (або) зберігання, то в структурі інформаційної сфери як основні об'єкти дії при інформаційному протиборстві виступають:

- мережі зв'язку і інформаційно-обчислювальні мережі, що використовуються державними організаціями при виконанні своїх управлінських функцій;
- військова інформаційна інфраструктура, що вирішує задачі управління військами;
- інформаційні і управлінські структури банків, транспортних і промислових підприємств;
- засоби масової інформації і, в першу чергу, електронні.

Інформаційну зброю можливо класифікувати по методах дії на інформацію, інформаційні процеси і інформаційні системи супротивника. Ця дія може бути фізичною, інформаційною, програмно-технічною або радіоелектронною.

Фізична дія може бути здійснена шляхом застосування будь-яких засобів вогневого ураження. Проте коректнішим було б віднести до інформаційної зброї фізичної дії засоби, призначені виключно для дії на елементи інформаційної системи: спеціалізовані акумуляторні батареї генерації імпульсу високої напруги, засоби генерації електромагнітного імпульсу, графітові бомби, біологічні і хімічні засоби впливу на елементну базу.

Інформаційні методи впливу реалізуються за допомогою всієї сукупності засобів масової інформації і глобальних інформаційних мереж типу Інтернет, станціями голосової дезінформації.

Атакуючою інформаційною зброєю сьогодні можна назвати:

- комп'ютерні віруси, здатні розмножуватися, упроваджуватися в програми, передаватися по лініях зв'язку, мережах передачі даних, виводити з ладу системи управління і т.п.;

- логічні бомби – програмні пристрої, які заздалегідь упроваджують в інформаційно-керуючі центри військової або цивільної інфраструктури, щоб по сигналу або у встановлений час привести їх в дію;

- засоби пригнічення інформаційного обміну в телекомунікаційних мережах, фальсифікації інформації в каналах державного і військового управління;

- засоби нейтралізації тестових програм;

- різного роду помилки, що свідомо вводяться супротивником в програмне забезпечення об'єкту.

Активна інформаційна зброя застосовується для нападу на інформаційні системи і підсистеми терористичних організацій і вірогідного супротивника.

Об'єктами поразки активною інформаційною зброєю можуть виступати:

- військове керівництво вірогідного супротивника;

- політичне керівництво вірогідного супротивника;

- лідери терористичних організацій;

- світова громадська думка при проведенні спеціальних інформаційно-психологічних операцій.

Інформаційно-психологічна дія є цілеспрямованою психологічною атакою на конкретні сфери психіки людини, групи осіб або суспільну свідомість в цілому. Дія може здійснюватися з використанням всього спектру методів і форм технічного, візуального, звукового, медикаментозного, фізичного, больового, віртуального придушення волі.

Інформаційна протидія є спеціальними комплексними контрзаходами, направленими на попередження, профілактику, випередження і захист від деструктивних задумів супротивника на розум людини, що приймає управлінські рішення.

Домінуючою метою операцій по інформаційній протидії є забезпечення безпеки власних інформаційних ресурсів. Мета досягається за рахунок фізичного захисту об'єктів, прихованого зовнішнього спостереження, технічної оснащеності, оперативного маскування, дезінформації у поєднанні з оперативними комбінаціями, контрпропагандою в комплексі з радіоелектронною боротьбою.

Одним з найбільш ефективних і новітніх засобів ведення інформаційного протиборства є електромагнітна зброя, призначена для дії на інформаційні системи. Масове застосування цієї зброї може порушити функціонування інформаційно-процесорної інфраструктури, паралізувати військові системи управління і життєво важливі виробництва супротивника, що значно понизить його боєготовність і ефективність проведення бойових операцій.

Оцінка фахівцями електромагнітної зброї як одного з найбільш ефективних засобів ведення інформаційного протиборства обумовлена високою значущістю інформаційних потоків в основних сферах діяльності людей – управлінні економікою, виробництвом, обороною країни. Порушення функціонування інформаційної системи, що забезпечує постійний обмін управлінськими рішеннями і включає безліч пристроїв збору і обробки інформації, викличе тяжкі наслідки.

Фундаментальний принцип інформаційного протиборства полягає в тому, що складні організаційні системи не можуть функціонувати без потоку інформації через їх структури. Інформація тече між цими структурами в декількох напрямах для типових умов функціонування. Припинення вихідного потоку інформації викличе параліч, оскільки команди не досягнуть елементів, які повинні їх виконати. Припинення вхідного потоку інформації ізолює елемент, що ухвалює рішення, від реальності і, таким чином, жорстко пригнічує його здатність ухвалювати раціональні рішення.

Універсальність, скритність, багатоваріантність форм програмно-апаратної реалізації, радикальність дії, достатній вибір часу і місця застосування, нарешті, економічність роблять інформаційну зброю надзвичайно небезпечною: вона легко маскується під засоби захисту, наприклад, інтелектуальної власності; вона дозволяє навіть вести наступальні дії анонімно, без оголошення війни.

Нормальна життєдіяльність суспільства цілком визначається рівнем розвитку, якістю функціонування і безпекою інформаційного середовища. Виробництво і управління, оборона і зв'язок, транспорт і енергетика, фінанси, наука і освіта, засоби масової інформації – все залежить від інтенсивності інформаційного обміну, повноти, своєчасності, достовірності інформації.

Саме інформаційна інфраструктура суспільства – мішень інформаційної зброї. Але в першу чергу інформаційна зброя націлена на збройні сили, підприємства оборонного комплексу, структури, відповідальні за зовнішню і внутрішню безпеку держави.

Темпи вдосконалення інформаційної зброї перевищують темпи розвитку технологій захисту. Тому задача нейтралізації інформаційної зброї повинна розглядатися як одна з пріоритетних в забезпеченні національної безпеки держави.

Для того щоб захиститися від загрози застосування інформаційної зброї перш за все необхідна оцінка загрози. Потрібний також періодичний аналіз геостратегічної ситуації з погляду вірогідності виникнення інформаційної війни. Ці оцінки і аналіз можуть служити основою для вироблення національної концепції протидії (нейтралізації) загрозі такої війни.

Таким чином, створення єдиного глобального інформаційного простору, що є природним результатом розвитку світової науково-технічної думки і вдосконалення комп'ютерних інформаційних технологій, створює передумови до розробки і застосування інформаційної зброї. Ефективне володіння інформаційною зброєю і засобами захисту від нього стає однією з головних умов забезпечення національної безпеки держави в XXI столітті.

Список літератури.

1. Панарин И. Н. Технология информационной войны/ И.Н. Панарин.–М.:“КСП+”, 2003.–320 с.
2. Прохожев А. А., Турко Н. И. Основы информационной войны, 1995.

УДК 004.9:32.019.51

Модель поведінки держави в умовах проявів ознак інформаційної експансії, агресії, війни

Доренський О.П., викладач
Кіровоградський національний технічний університет, м. Кіровоград

Інформація, яка визначається як сигнали або відомості, сприйняті приймачем та перетворені у сигнали керування [1], сьогодні активно використовується як ефективний інструмент досягнення суспільно-політичних, економічних, геополітичних цілей держави, а за допомогою сучасних інформаційних технологій перетворена на потужну зброю масового ураження. Адже боротьба держав в інформаційному просторі ведеться за зони політичного й економічного впливу, джерела сировини, ринки збуту й території, а всередині країни – за владу, власність, політичний вплив, можливість маніпулювати настроями й поведінкою громадян [2]. Означене призвело до появи й активного ведення війн нового покоління – інформаційних (ІВ), під якими розуміють проведення широкомасштабних інформаційних

дій, що застосовуються сторонами, які знаходяться у протиборстві, направлених проти соціальних та інформаційно-технічних систем держави з метою одержання інформаційної переваги над противником [3]. Вони стали несиловим засобом забезпечення державами власних інтересів та вирішальним фактором в досягненні результатів.

На сьогодні ІВ є ефективним засобом оволодіння ресурсами за допомогою механізмів агітації, пропаганди й інформаційного протистояння [2], що здійснюється у формах (ступенями) інформаційної експансії, інформаційної агресії та інформаційної війни [4, 9].

Відповідно до класифікації [5] ІВ є війнами сьомого покоління. Її поява стала наслідком наступних чинників:

– розвиток засобів обчислювальної техніки і комунікації [2];

– розвиток прикладної психології у сфері вивчення поведінки людей та управління їх мотиваціями [2, 6];

– глобалізація та масштабна інформатизація суспільства.

Предметом інформаційної війни є впливи на об'єкти. Серед багатьох їх різновидів під час ведення ІВ ключовим є інформаційний [7], надефективність якого забезпечують:

– активне впровадження у фахову діяльність й повсякденне життя людей електронних інфокомунікаційних систем, соціальних мереж, мобільних пристроїв тощо;

– інтеграція у життя й виникнення стійкої залежності сучасної людини від інформаційно-телекомунікаціних, мережевих, мобільних засобів тощо, які стають основним джерелом інформації, а, отже, формують думку, світогляд та поведінку громадськості.

Водночас, спостерігається стрімке вдосконалення засобів ведення інформаційної боротьби. Першочергово це стосується інформаційної зброї, яка призначена для боротьби з комп'ютерними мережами і системами управління. До сучасної інформаційної зброї входить сукупність спеціально організованої інформації та інформаційних технологій, що дозволяє цілеспрямовано змінювати, знешкоджувати, копіювати, блокувати інформацію, долати системи захисту, здійснювати дезінформацію, пошкоджувати функціонування носіїв інформації, інфокомунікаційних систем та мереж [8].

Отже, з означеного випливає, що актуальною задачею є постійний моніторинг відповідними органами держави проявів ознак інформаційної експансії, агресії, війни [9] або їх гібридів, яку слід сприймати як пряму загрозу національній безпеці та невідкладно вживати належних заходів і застосування засобів інформаційної протидії й захисту. Таким чином, метою роботи є розроблення моделі адекватної поведінки держави (її відповідних органів) на ранніх стадіях інформаційної експансії, агресії, війни або їх гібридних форм.

Задля захисту інформаційного простору держави в умовах проявів ознак інформаційної експансії, агресії або війни слід вжити заходів нейтралізації й знищення інформаційного ресурсу противника та захисту власного інфоресурсу. Реалізувати означене можливо за допомогою інформаційно-ударної операції [10]. Її базовими задачами є:

– забезпечення інформаційної переваги шляхом активного впливу на системи державного і військового управління противника та на джерела інформаційних загроз;

– введення противника в оману стосовно операції, яка проводиться;

– зниження морально-психологічної стійкості та бойового духу особового складу противника;

– протидія негативному інформаційному впливу противника.

Інформаційно-ударна операція проводиться на основі [11]:

– використання сучасних інформаційних та телекомунікаційних засобів, технологій, соціальних мереж тощо;

– застосування військових засобів;

– демонстрація вогневої могутності сучасної зброї, передислокація військ;

– висвітлення та характеристика в засобах масової інформації об'єктів ураження;

– організація потоків біженців та провокації громадських зіткнень;

– цілеспрямований вплив на суспільну думку щодо несприйняття противника, блокування кордонів, введення ембарго на поставку військової та інших видів

продукції противника;

– масове використання безпілотних літальних апаратів та високоточної зброї;
– висвітлення подій у світових інформаційно-телекомунікаційних мережах;
– знищення військово-стратегічних цілей.

Отже, за результатами дослідження запропоновано та в доповіді презентується модель поведінки держави в умовах проявів ознак інформаційної експансії, агресії, війни або їх гібридів. Її сутність полягає у здійсненні постійного моніторингу інформаційного простору, виявлення ознак інформаційного противника та невідкладне проведення інформаційно-ударної операції з метою протидії й захисту власних ресурсів на ранніх стадіях інформаційної експансії, агресії або війни. Означене дасть істотну перевагу у випадку ведення ІВ, можливість мінімізувати витрати на інформаційне протистояння, унеможливлення часткової або повної втрати політичного стану, ресурсів, а також забезпечення захисту суспільства, національного інтересу й держави в цілому.

Список літератури

1. Притула А.В. Природа інформації та її визначення / А.В. Притула, В.Я. Решетник // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій : IV Міжнар. наук.-прак. конф., 24-26 кві, 2008 р. : тези доп. – Запоріжжя, 2008. – С. 114-115.

2. Шумка А.В. Інформаційно-мережева війна – нова форма міждержавного протиборства початку XXI ст. / А.В. Шумка, П.П. Черник // Військово-науковий вісник. – 2013. – Вип. 19. – С. 243-255.

3. Медведєв В.К. Сучасна інформаційна війна та її обрис / Медведєв В.К., Кучеренко Ю.Ф., Гузько О.М. // Системи озброєння і військова техніка. – 2008. – № 1(13). – С. 52-54.

4. Пілат М. Інформаційні впливи та інформаційні війни: сутність понять та їхній взаємозв'язок в інформаційну епоху / Марина Пілат // Вісник Львівського університету. – 2013. – Вип. 32. – С. 185-190.

5. Слипченко В. Природа войны: вчера, сегодня, завтра / В.Слипченко. – М.: Третий Рим, 2004. – 196 с.

6. Сенченко О. Новітні війни з використанням інформаційно-психологічної зброї / Оксана Сенченко // Вісник Книжкової палати. – 2014. – № 8. – С. 1-6.

7. Воробйова І.В. Інформаційно-психологічна зброя як самостійний засіб ведення інформаційно-психологічної війни / І.В. Воробйова // Системи озброєння і військова техніка. – 2010. – № 1(21). – С. 141-144.

8. Кучеренко Ю.Ф. Погляди на ведення інформаційної боротьби в сучасних війнах / Кучеренко Ю.Ф., Гордієнко В.М., Гузько О.М. // Системи озброєння і військова техніка. – 2011. – № 3(27). – С. 108-111.

9. Мануйло А. В. Государственная информационная политика в условиях информационно-психологической войны. / А.В. Манойло, А.И. Петренко, Д.Б. Фролов. – М.: Горячая линия, 2003. – 541 с.

10. Гриняев С. Концепция ведения информационной войны в некоторых странах мира / Сергей Гриняев // Зарубежное военное обозрение. – 2002. – №2. – С. 11-16.

11. Войтко О.В. Передумови створення концепції інформаційної війни в еру новітніх технологій / О.В. Войтко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2013. – № 3(18). – С. 99-100.

УДК 004.056.55

Інформаційні війни: поняття, мета, завдання та їх значення

Кліпа О.С., курсант 4 курсу
Науковий керівник – Безрученко В.С., канд. фіз.-мат. наук, доцент
Національний університет державної податкової служби України, м. Ірпінь

Інформаційна війна – використання і управління інформацією з метою набуття конкурентоздатної переваги над супротивником.

Інформаційна війна може включати в себе:

- збір тактичної інформації,

- забезпечення безпеки власних інформаційних ресурсів,
- поширення пропаганди або дезінформації, щоб деморалізувати військо та населення ворога,
- підрив якості інформації супротивника і попередження можливості збору інформації супротивником.

У книзі Прокофьєва «Інформаційна війна і інформаційна злочинність» визначається: інформаційна війна – це дії, початі для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації і інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації і інформаційних системах.

В праці з теорії інформаційної війни 1995 р. Шафранські напише: «*Система цілей інформаційної війни може включати кожен елемент епістемології супротивника*». Тобто будь-що в його системі знань може стати такою ціллю.

Дж. Стейн у тому ж 1995 р. друкує розвідку «Інформаційна війна», де теж акцентує, що інформаційна війна має справу з ідеями та епістемологією. Стосовно більш конкретних цілей він стверджує наступне: «*Метою інформаційної війни є людський розум, особливо той, який приймає ключові рішення війни та миру, а також той, що приймає ключові рішення стосовно того, де, коли та як застосувати потенціал і можливості, які є в їхніх стратегічних структурах*».

Тобто ми бачимо, що тоді, в 1995 р., інформаційна війна уявлялася навіть більш складним феноменом, ніж ми розуміємо її зараз. Чітко наголошується, що метою є розум супротивника. Вона є не війною інформації, як сьогодні, а війною знань. І це є найближчим завданням розвитку цієї сфери. Хоча ми можемо визнати, що, наприклад, Перебудова була якраз війною знань, коли базові знання та цінності були замінені в цілої країни.

Австралійській підполковник **Д. Коннері** теж бачить майбутню війну як війну знань. Він акцентує, що окрім фізичного та інформаційного існує ще й когнітивний вимір. Саме там відбувається людське мислення. Коннері вважає, що війна знань створює події чи інформацію, які не відповідають очікуванням опонента, ведучи його до розуміння того, що ціна конфлікту є дуже високою й не виправдовує перемоги. Косово та Ірак, на його думку, демонструють деякі аспекти війни знань.

Часто інформаційна війна ведеться в комплексі з кібер- та психологічною війнами з метою ширшого охоплення цілей, із залученням радіоелектронної боротьби та мережевих технологій.

Сучасні війни ведуться перш за все в інформаційній сфері, яка випереджає і безперервно супроводжує так званий «прямий контакт» протиборчих сторін. Якщо торкнутися цього питання на міждержавному рівні, то ми побачимо, що спецслужби країн ведуть свої війни безпосередньо в Інтернеті. Як повідомлялося, для боротьби з потенціальним супротивником в експортне мережене обладнання США встановлюються чіпи з логічними вірусами, які можуть бути активовані в потрібний момент. Для боротьби з певними людьми є комп'ютерні програми обнуління банківських рахунків. Для боротьби між корпораціями, які є конкурентами на різних ринках використовується промислове шпигунство, яке полягає у зборі інформації щодо свого «супротивника» (майбутні плани, поточні справи, фінансове становище).

Виходячи зі змісту та ролі інформації у сучасному світі, американський дослідник Маклюен М. виводить цікаву тезу, що звучить так: «Істинно тотальна війна – це війна за допомогою інформації».

Мета інформаційної війни – послабити моральні і матеріальні сили супротивника або конкурента та посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях. Очевидно, що інформаційна війна – складова частина ідеологічної боротьби. Вони не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою. І це породжує небезпечну безпечність у ставленні до них. Тим часом, руйнування,

яких завдають інформаційні війни у суспільній психології, психології особи, за масштабами і за значенням цілком співмірні, а часом і перевищують наслідки збройних воєн.

Головне завдання інформаційних воєн полягає у маніпулюванні масами. Мета такої маніпуляції найчастіше полягає у:

- внесенні у суспільну та індивідуальну свідомість ворожих, шкідливих ідей та поглядів;
- дезорієнтації та дезінформації мас;
- послабленні певних переконань, устоїв;
- залякуванні свого народу образом ворога
- залякуванні супротивника своєю могутністю. Нарешті, останнє, але не менш важливе завдання: забезпечення ринку збуту для своєї економіки. У цьому випадку інформаційна війна є складовою частиною конкурентної боротьби.

Інформаційна війна розглядає інформацію як окремий об'єкт або як потенційну зброю та вигідну ціль. Інформаційну війну можна розглядати як якісно новий вид бойових дій, активна протидія в інформаційному просторі. Інформаційна війна – це атака інформаційної функції, незалежно від засобів, які застосовуються.

У веденні стратегічних інформаційних війн застосовується специфічна зброя. Ця зброя не наносить фізичної шкоди, але може призвести до справжньої війни.

Інформаційна зброя – сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій або служб інформаційної інфраструктури в цілому або окремих її елементів (рис.1).

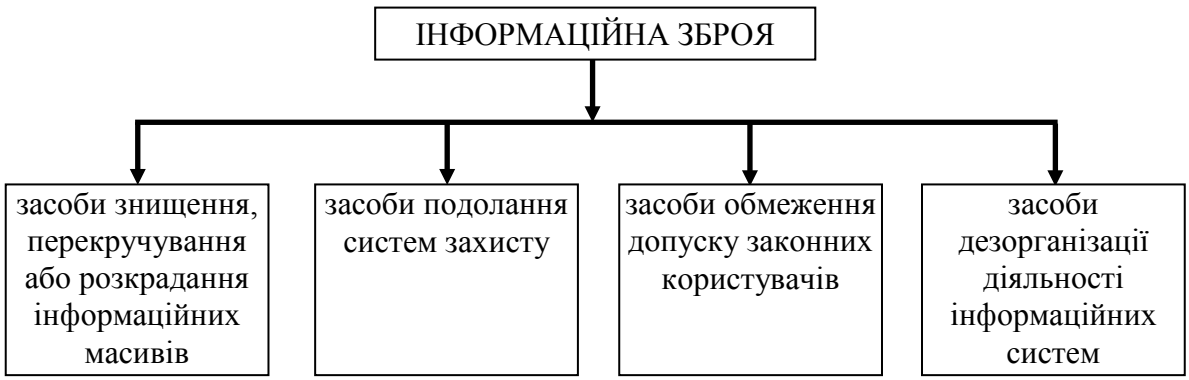

Рисунок 1 – Засоби інформаційної зброї [3]

Основна дія інформаційної зброї – блокування або спотворення інформаційних потоків та процесів прийняття рішень супротивника.

Прикладом інформаційних війн на сучасному етапі може бути російсько-грузинський конфлікт 2008 року.

Від часу проголошення незалежності України Російська Федерація веде постійну інформаційну війну проти України. Особливо вона була інтенсифікована в роки правління проросійського режиму Януковича. Від початку агресії Російської Федерації (лютий 2014) російська пропаганда набула форм геббельсівської пропаганди часів Другої світової війни.

У Російській Федерації на всіх рівнях суспільства розгорнута пропаганда війни.

Інформаційну війну, що є інформаційним забезпеченням агресії Російської Федерації проти України, відомий російський політик Борис Нємцов охарактеризував як війну нацистського режиму проти демократичної держави: «Виграти війну можуть нацисти із Геббельсом на чолі. Те, що Україна програла інформаційну війну – це факт. Але те, що ви не повинні з цього приводу дуже переживати – це теж факт. Ви ж не нацистська держава», –

сказав російський опозиціонер.

Необхідний безперервний і послідовний моніторинг загроз, пов'язаних з можливим розв'язанням інформаційної війни, з постійною і тверезою оцінкою можливостей протидії, нейтралізації і запобігання цих загроз. На думку фахівців, моніторинг повинен охоплювати:

- динаміку внутрішньої та зовнішньополітичної ситуації, глобальні і локальні протиріччя та конфлікти;
- науково-технічний прогрес у сфері розробки заходів і методів проникнення в інформаційні ресурси і впливи на інформаційну інфраструктуру, а також в області захисту інформації;
- стан внутрішнього і міжнародного законодавчо-правового забезпечення інформаційної безпеки;
- стан і ефективність систем забезпечення інформаційної безпеки.

Ідеальну схему організації моніторингу можна представити у вигляді ієрархічної структури, вищою ланкою якої є надвідомчий повноважний орган (РНБОУ), куди від міністерств, відомств і власних джерел надходить інформація про стан безпеки об'єктів і систем. Аналіз цієї інформації дозволить оцінювати і прогнозувати ситуацію по забезпеченню безпеки, здійснити координацію діяльності і сформувати плани розвитку системи безпеки в цілому. Реалізація подібної схеми моніторингу в даний час ускладнена, тому що забезпеченням інформаційної безпеки сьогодні змушені займатися різні державні відомства, насамперед силові міністерства. Щоб такого роду «мозаїчний» конгломерат окремих відомчих підсистем функціонував досить успішно й ефективно, повинні бути погоджені їхні зусилля і скоординована їхня діяльність, насамперед, на нормативно-правовому і методичному рівнях. Організаційне забезпечення ідеологічного об'єднання підсистем інформаційної безпеки, як це приблизно зроблено в США або Франції, могла б взяти на себе Рада національної безпеки й оборони України.

Список літератури

1. Вікіпедія. Інформаційна війна [Електронний ресурс]. – Режим доступу: uk.wikipedia.org/wiki/Інформаційна_війна
2. Вікіпедія. Російська інтервенція до Криму 2014 [Електронний ресурс]. – Режим доступу: uk.wikipedia.org/wiki/Російська_інтервенція_до_Криму_2014
3. Інформаційні війни та майбутнє України [Електронний ресурс]. – Режим доступу: http://siac.com.ua/index.php?option=com_content&task=view&id=1054&Itemid=44
4. Почепцов Г.Г. Інформаційні війни: тенденції та шляхи розвитку [Електронний ресурс]. – Режим доступу: http://osvita.mediasapiens.ua/ethics/manipulation/informatsiyni_viyni_tendentsii_ta_shlyakhi_rozvitku/
5. Бабенко Ю. Інформаційна війна – зброя масового знищення! [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/rus/articles/2006/04/20/4399050/

УДК 007.304.659.3

Огляд основних форм інформаційного протиборства

Колісніченко О.Ю., студент 2 курсу
Науковий керівник – Минайленко Р.М., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Вступ

На сьогоднішній день інформація відіграє чи не найважливішу роль в житті людей, вона стала невід'ємною частиною нашого життя. Інформація стала у XXI столітті регулятором усіх суспільних, політичних, економічних та соціальних відносин. Процес інформатизації розвивається настільки стрімко, що веде до створення єдиного

інформаційного простору. Це є позитивним для людства, адже швидкий обмін економічною, політичною, технічною та іншими видами інформації дозволяє людству швидко розвиватися. Однак, створення інформаційного суспільства може привести до виникнення багатьох інформаційних катастроф, руйнування духовності суспільства і приведення до великомасштабних технічних катастроф.

Саме негативні прояви інформаційного суспільства породжують таке поняття, як "інформаційна війна", яка сьогодні стала реальною загрозою безпеці людства. Спостерігаючи за ходом і наслідками війн та конфліктів XX та XXI століть, ми бачимо, що роль інформаційного забезпечення різко зростає, і свідчить про новий рівень ведення інформаційного протиборства. Інформаційна війна включає в себе багато аспектів, основними з яких є вплив на свідомість людини різними нейролінгвістичними засобами, які полягають в підриві цілей та світогляду людей.

Таким чином інформаційна війна сьогодні є всеосяжною, цілісною стратегією, яка показує всю значимість володіння інформацією в керуванні, командуванні і реалізації національної політики. Інформаційна війна стає війною за знання, за те кому будуть відомі відповіді на найважливіші питання, що дають змогу керувати масами. Звичайно, при веденні такої війни кількість жертв зводиться до мінімуму, але участь у ній беруть безпосередньо усі люди, що може привести до руйнування соціуму, як такого.

Поняття та зміст інформаційного протиборства

Інформаційне протиборство - суперництво соціальних систем (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку.

За інтенсивністю, масштабами та засобами, які використовуються, виділяють наступні ступені інформаційного протиборства: інформаційна експансія, інформаційна агресія та інформаційна війна.

Інформаційна експансія це діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу а метою:

- поступова, плавна, непомітна для суспільства зміна системи соціальних відносин за зразком системи джерела експансії;
- витіснення положень національної ідеології і національної системи цінностей і заміщення їх власними цінностями й ідеологічними установками;
- збільшення ступеню свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою та національними ЗМІ;
- нарощування присутності власних ЗМІ в інформаційній сфері об'єкта проникнення і т.п.

Інформаційна агресія - незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретної, відчутної шкоди в окремих областях його діяльності шляхом обмеженого та локального по своїх масштабах застосування сили.

Основними ***формами інформаційного протиборства*** на державному рівні є:

- політичні, дипломатичні й економічні акції;
- інформаційні та психологічні операції;
- підривні та деморалізуючі пропагандистські дії;
- сприяння опозиційним і дисидентським рухам;
- надання усебічного впливу на політичне і культурне життя з метою розвалу національно-державних підвалин суспільства;
- проникнення в систему державного керування.

На воєнному рівні термін інформаційна боротьба можна порівняти з радіоелектронною або психологічною боротьбою. Інформаційна боротьба визначається як комплекс заходів, які впроваджуються в масштабах ЗС для досягнення інформаційної

переваги над противником шляхом впливу на інформацію, якою він володіє, процеси, що залежать від інформації, інформаційні системи, комп'ютерні мережі з одночасним захистом від аналогічних впливів з боку противника. Виділяються наступальна й оборонна складові інформаційної боротьби.

Інформаційна війна

Сьогодні інформація добирає матеріальну форму і володіння нею стає дуже жаданим. До реалізації будь-які, цілком "матеріальні", рішення сьогодні випробуються в інформаційній області. І результати стають вирішальними.

Сучасні війни ведуться перш за все в інформаційній сфері, яка випереджає і безперервно супроводжує так званий "прямий контакт" супротивників. Якщо торкнутися цього питання на міждержавному рівні, то ми побачимо, що спецслужби країн ведуть свої війни безпосередньо в Інтернеті. Як повідомлялося, для боротьби з потенціальним супротивником в експортне мережеве обладнання США встановлюються чіпи з логічними вірусами, які можуть бути активовані в потрібний момент. Для боротьби з певними людьми є комп'ютерні програми обнулення банківських рахунків. Для боротьби між корпораціями, які є конкурентами на різних ринках, використовується промисловий шпіонаж, який полягає у зборі інформації щодо свого "супротивника" (майбутні плани, поточні справи, фінансове становище) і т.д.

Виходячи зі змісту та ролі інформації у сучасному світі, американський дослідник М. Маклюен виводить цікаву тезу, що звучить так: "Істинно тотальна війна - це війна інформаційна".

Саме Маклюен першим (ще 30 років тому) проголосив, що в наш час економічні зв'язки і відносини усе більше приймають форму обміну знаннями, а не обміну товарами. А засоби масової комунікації самі є новими "природними ресурсами", що збільшують багатства суспільства. Тобто боротьба за капітал, простори збуту та інше йдуть на другий план, а головним зараз є доступ до інформаційних ресурсів і знань. Це призводить до того, що війни ведуться вже більше в інформаційному просторі та за допомогою інформаційних видів озброєнь.

Інформаційний тероризм

В сучасному світі існує багато способів маніпуляції завдяки інформації. Маніпулятивні технології набувають дедалі ширшого використання, завдяки їм ведуться інформаційні війни, знищення опонентів (конкурентів), вплив на маси і багато інших дій. Але останнім часом великої популярності набув інформаційний тероризм.

На відміну від інформаційних війн терористичні акти одноразові і мають знищуючу силу. Частіше в таких випадках інформаційні терористи мають на меті тільки одне – досягти якомога швидше потрібної мети і наробити побільше галасу.

Медіа-інформаційний тероризм є особливим різновидом психологічного терору, який відносять до інфраструктурного, а саме - зловживання інформаційними системами, мережами та їх компонентами для здійснення терористичних дій та інших віднесених до них акцій.

Такий різновид тероризму характеризується як множина інформаційних війн та спеціальних операцій, пов’язаних із національними або транснаціональними кримінальними структурами і спецслужбами іноземних держав. Інформаційний тероризм здійснюється в області, що охоплює політичні, філософські, правові, естетичні, релігійні й інші погляди й ідеї, тобто в духовній сфері, там, де ведеться боротьба ідей. Доступність інформаційних технологій значно підвищує ризики інформаційного тероризму, бо, чим інформатизованішим є суспільство, тим більш воно піддатливе до впливів масово-психологічного терору.

Інформаційний тероризм - це, насамперед, форма негативного впливу на особистість, суспільство і державу усіма видами інформації. Його ціль - ослаблення і розхитування конституційного ладу. Він ведеться різноманітними силами і засобами - від агентури іноземних спецслужб до вітчизняних і закордонних ЗМІ.

Висновок

Спираючись на те, що у сучасному світі найбільше влади має той, хто контролює інформацію якою ми користуємося, я вважаю, що просто необхідним є розвиток систем інформаційної безпеки і протиборства інформаційному тероризму, адже саме вони є причиною усіх сучасних інформаційних та збройних війн, які забирають сотні людських життів і отруюють душі мільйонів.

Список літератури

1. Панасенко С.П., Защита информации в компьютерных сетях // Журнал "Мир ПК" 2002 № 2.
2. Інформаційна війна: Матеріал з Вікіпедії – вільної енциклопедії // http://uk.wikipedia.org/wiki
3. Афанасьєв В. Соціальна інформація та управління суспільством. – М.: Знание, 2005.
4. Блек С. Паблик рилейшнз. Що це таке? – М.: Наука, 2007.
5. Вершинін М.С. Політична комунікація в інформаційному суспільстві – М.: Ягуар, 2006.
6. Бабенко Ю. Інформаційний тероризм // Інститут масової інформації – http://olden.imi.org.ua/node/18257

УДК 32.019.51:004.056.5

Методи протидії деструктивним інформаційним впливам в соціальних мережах в умовах інформаційної війни

Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

З 2014 року Російська Федерація розпочала гібридну війну з Україною, основними складовими якої являються: анексія Криму в березні 2014 та збройний конфлікт на частині територій Донецької та Луганської областей з квітня 2014.

27 січня 2015 року Верховна Рада України визнала у своїй заяві-зверненні до міжнародних організацій Російську Федерацію країною-агресором [1].

Гібридна війна – це військова стратегія, що поєднує звичайну війну, розвідувальні, диверсійні, партизанські і терористичні дії малих підрозділів, кібервійну, інформаційну та психологічну війну.

Надзвичайно важливою та деструктивною складовою російської агресії проти України стала саме інформаційна війна.

Складові інформаційної війни:

- шпигунство та викрадення інформації супротивника;
- поширення пропаганди та/або дезінформації;
- псування інформації супротивника, блокування ресурсів, підміна інформації.

Одним з засобів інформаційної війни стало поширення пропаганди та дезінформації через СМІ та соціальні мережі. Розповсюджувачами пропаганди стали як відомі люди – блогери, журналісти, артисти тощо, так і боти та аноніми. Завдяки російській групі хакерів "Анонімний інтернаціонал" стало відомо про створення організацій (наприклад, ТОВ "Інтернет дослідження" з офісом в Ольгіно, м. Санкт-Петербург), що займалися поширенням пропаганди та дезінформації через платні публікації та коментарі в соціальних мережах. Електронні скриньки керівників цієї організації були зламані, а листи викладені у мережу Інтернет [2]. Згодом на основі даної переписки були проведені журналістські розслідування та навіть взяті інтерв'ю у людей, що в минулому працювали там платними коментаторами

[4, 5]. В [4] зазначається, що в ТОВ "Інтернет дослідження" приблизно 250 чоловік, змінюючи один одного раз в 12 годин, безперервно писали в соціальних мережах, в основному в "Живий журнал" та "ВКонтакті", причому одні писали пости, а інші їх коментували для підняття рейтингу.

Ця тактика не нова, в Китаї вже давно існує армія платних коментаторів, так звана Умаодан, або "50-центова армія", що складається з китайських провладних блогерів та учасників Інтернет-форумів, які пишуть тексти та коментарі за гроші для формування громадської думки в тому чи іншому напрямку. Умаодан за деякими оцінками складає 300 тисяч чоловік [5].

Як показує досвід, подібні платні блогери та коментатори здатні вносити значний деструктивний інформаційний вплив та маніпулювати громадською думкою, що становить небезпеку для інформаційної безпеки держави.

В ряді наукових робіт показано, що міркування людей в соціальній мережі в значній мірі залежать від міркувань впливових учасників даної мережі, яким вони довіряють, а також від міркувань більшості [6, 7, 8], так як самі вони не мають достатньої кількості інформації для формування повністю об'єктивної думки. Тому для зміни громадської думки достатньо переконати або підкупити лише невелику кількість користувачів, які потім переконають інших в потрібній інформації, і/або створити видимість одностайності більшості в якомусь питанні завдяки великій кількості фейкових акаунтів. В роботі [9] показана модель вірусного поширення інформації в соціальній мережі. Варто зауважити, що "антивірусів" для таких інформаційно-соціальних вірусів поки що не існує.

Дехто може вважати, що інформаційна війна та інформаційні впливи не призводять до такої кількості смертей як реальні бойові дії, але це хибна думка. Так в 2014 році науковець Девід Янагізава-Дротт написав статтю [10] у якій розглянув геноцид у Руанді 1994 року, в якому активісти-хуту за допомогою мачете і голими руками за 3 місяці вбили 500 тисяч тутсі (а за деякими джерелами близько мільйона), та знайшов кореляцію між зонами, де приймалася радіостанція «Радіо Тисячі Пагорбів» з пропагандиськими націоналістичними передачами та зонами де було вбито найбільшу кількість тутсі. В зоні впевненого прийому радіостанції було вбито на 62-69% людей більше, ніж там, де сигналу не було зовсім.

Існує багато наукових робіт з аналізу соціальних мереж та методів інформаційного впливу на їх користувачів з різними цілями від маркетингових до політичних [6, 7, 8, 12], але в той же час дуже мало напрацювань стосовно того, як протидіяти даним інформаційним впливам. Хоча навіть невеликими зусиллями можна виявити деструктивні втручання в соціальні мережі. Наприклад, відразу після вбивства російського опозиційного політика Бориса Нємцова американський журналіст Алек Лун помітив, як велика кількість користувачів Твіттеру розмістили однакові твіти. Йшлося про те, що Нємцова вбили українці. За допомогою відкритих онлайн-інструментів NodeXL та Gephi інтернет-дослідник Лоуренс Александер зібрав та візуалізував дані про користувачів, що поширювали дану інформацію та виявив понад 20 тисяч прокремлівських ботів серед твіттер-аккаунтів [11].

Сучасні способи поширення пропаганди та дезинформації ставлять перед суспільством нові виклики, адже не існує чітких та добре працюючих механізмів захисту від деструктивного інформаційного впливу на суспільство через соціальні мережі.

Аналіз величезних масивів інформації та дій сотень тисяч користувачів не представляється можливим здійснювати лише з використанням людських ресурсів без втрати якості, швидкості та відсутності помилок суб'єктивного сприйняття. До того ж читати великі масиви деструктивної інформації може бути шкідливо для людської психіки. Автоматично розпізнавати агентів впливу в соціальних мережах програмними засобами видається досить перспективним методом, що дозволить оперативно відслідковувати та спростовувати фейкову інформацію, а також викривати або блокувати таких агентів і опубліковані ними матеріали.

В даній роботі була поставлена мета дослідити можливі методи виявлення джерел поширення деструктивних впливів в соціальних мережах та способи протидії їм.

Методи протидії деструктивним впливам в соціальних мережах мають включати в себе:

1) методи виявлення загроз;

2) методи нейтралізації загроз.

Було проаналізовано існуючі методи аналізу соціальних мереж та методи аналізу даних, напр., [7, 11, 12, 13, 14], з метою виявлення таких, за допомогою яких можливо виявляти деструктивні інформаційні впливи на користувачів.

Для виявлення деструктивних впливів в соціальних мережах доцільно використовувати наступні методи та засоби:

- кластеризація даних;
- класифікація даних;
- колаборативна фільтрація;
- експертні системи;
- нейронні мережі;
- штучні імунні системи;
- лінгвістичний аналіз текстів;
- інформаційний пошук;
- когнітивне моделювання;
- стеганографічні методи виявлення джерел поширення інформації - технологія "цифрових відбитків пальців".

Дані методи та засоби дозволять отримувати наступну інформацію про соціальні мережі та їх інформаційне наповнення:

- виділення спільнот у соціальній мережі, що поширюють деструктивну інформацію;
- виявлення спаму;
- виявлення фейкових аккаунтів та ботів;
- виявлення різних профілів одного користувача;
- виявлення лідерів думок, через яких впливають на загальну думку;
- оцінка інформаційних впливів у соціальній мережі;
- побудова тематичного профілю інтересів користувача або групи користувачів;
- визначення прихованих атрибутів користувачів за текстами їх повідомлень;
- визначення емоційного забарвлення повідомлень;
- виявлення мовних конструкцій, характерних для НЛП та інших методик маніпулювання громадською думкою;
- визначення структури спільнот (ієрархічні, мережні, слабкозв’язні, сильнозв’язні тощо);
- виявлення джерел поширення деструктивної інформації;
- виявлення шляхів поширення деструктивної інформації
- і т.д.

Параметри, за якими можна проводити аналіз соціальних мереж:

- граф зв’язків між користувачами;
- хештеги;
- лайки;
- репости, ретвіти;
- списки спільнот та діячів, на які користувач підписаний;
- найбільш часто зустрічаємі слова, словосполучення, фрази у постах, коментарях тощо.

В якості методів нейтралізації загроз доцільно використовувати наступні:

- інформування користувачів про виявлені загрози;
- спростовування виявленої дезінформації;
- блокування екстремістських матеріалів, фейкових аккаунтів, ботів;
- фільтрація спаму;
- зміна політик безпеки;
- захист лідерів думок від деструктивного впливу, своєчасне надання їм достовірної та

актуальної інформації;

- своєчасне надання актуальної інформації користувачам соціальної мережі;
- підвищення освіченості людей у сфері інформаційної безпеки.

Висновок. В роботі було здійснено огляд загроз інформаційній безпеці держави в соціальних мережах. Проведено дослідження методів аналізу соціальних мереж та аналізу даних з метою виявлення таких, що можна використати для виявлення деструктивних інформаційних впливів в соціальних мережах. А також запропоновано методи нейтралізації деструктивних інформаційних впливів.

Список літератури

5. Постанова Верховної Ради України. Про Звернення Верховної Ради України до Організації Об'єднаних Націй, Європейського Парламенту, Парламентської Асамблеї Ради Європи, Парламентської Асамблеї НАТО, Парламентської Асамблеї ОБСЄ, Парламентської Асамблеї ГУАМ, національних парламентів держав світу про визнання Російської Федерації державою-агресором. № 129-19 від 27.01.2015

6. Блог российской хакерской группы Анонимный интернационал (также известен как «Шалтай-Болтай») [Електронний ресурс]. – Режим доступу: http://b0ltai.org/

7. Гармажапова А. Где живут тролли. И кто их кормит. http://www.novayagazeta.ru/politics/59889.html [Електронний ресурс]. – Режим доступу: http://www.novayagazeta.ru/politics/59889.html

8. Тролли из Ольгино переехали в новый четырехэтажный офис на Савушкина [Електронний ресурс]. – Режим доступу: http://www.dp.ru/a/2014/10/27/Borotsja_s_omerzeniem_mo/

9. Malik Fareed China joins a turf war [Електронний ресурс]. – Режим доступу: http://www.theguardian.com/media/2008/sep/22/chinathemedia.marketingandpr

10. Губанов Д.А. Модели информационного влияния и информационного управления в социальных сетях / Д.А. Губанов, Д.А. Новиков, А.Г. Чхартишвили // Проблемы управления. – Вып. № 5. – М.: ИПУ РАН. – 2009. – Стр. 28-35

11. Губанов Д.А., Новиков Д.А., Чхартишвили А.Г. «Социальные сети: модели информационного влияния, управления и противоборства». – М.: МЦНМО – 2010. – 228 стр.

12. Колодин Д.В. Информационное влияние в социальных сетях в виртуальной реальности // Вестник ЧелГУ . 2014. №11 (340). [Електронний ресурс] – Режим доступу: http://cyberleninka.ru/article/n/informatsionnoe-vliyanie-v-sotsialnyh-setyah-v-virtualnoy-realnosti

13. Кристина Лерман, Руми Жош, Таван Сурачавала Социальное заражение: исследование распространения информации с помощью пользовательских графов на ресурсах Digg та Twitter [Електронний ресурс] – Режим доступу: http://webscience.ru/details/socialnoe-zarazhenie-issledovanie-rasprostraneniya-informacii-s-pomoshchyu-polzovatelskih

14. David Yanagizawa-Drott Propaganda and Conflict: Evidence from the Rwandan Genocide - 10.2014 Quarterly Journal of Economics 129(4) [Електронний ресурс] – Режим доступу: http://www.hks.harvard.edu/fs/dyanagi/Research/RwandaDYD.pdf

15. Lawrence Alexander Social Network Analysis Reveals Full Scale of Kremlin's Twitter Bot Campaign [Електронний ресурс]. – Режим доступу: http://globalvoicesonline.org/2015/04/02/analyzing-kremlin-twitter-bots/

16. Сегаран Т. Программируем коллективный разум. – Пер. с англ. – СПб: Символ-Плюс, 2008. – 368 с.

17. Social Network Analysis: Theory and Applications [Електронний ресурс] – Режим доступу: train.ed.psu.edu/WFED-543/SocNet_TheoryApp.pdf

18. Коршунов А. и др. Анализ социальных сетей: методы и приложения // Труды ИСП РАН – Вып. № 1, том 26. – 2014 [Електронний ресурс] – Режим доступу: http://cyberleninka.ru/article/n/analiz-sotsialnyh-setey-metody-i-prilozheniya#ixzz3XKTa5dLe

УДК 004.056.5:32.019.51

Огляд методів інформаційної війни

Таран Р.А., студент 4 курсу
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет, м. Кіровоград

Інформаційна війна - цілеспрямовані дії, вжиті для досягнення інформаційної переваги шляхом завдання шкоди інформації, інформаційним процесам та інформаційним

системам противника при одночасному захисті власної інформації, інформаційних процесів та інформаційних систем.

Інформаційна війна має атакувальні і захисні складові, але починається з цільового проектування і розробки своєї архітектури командування, управління. Методами інформаційної війни є подання дезінформації, або подання інформації, яка є вигідною для себе.

В інформаційній війні можна виділити декілька етапів:

- визначення цілей;
- визначення стратегії, яка повинна враховувати: підготовку повідомлення, визначення каналу комунікації та цільової аудиторії, вибір комунікатора;
- складання плану тактичних засобів.

Згідно цим етапам обирається один або декілька методів, які найбільш підходять для заданих цілей. Розглянемо деякі з методів ведення інформаційної війни.

Використання авторитетів (груп впливу). Метод полягає у використанні авторитетних, відомих для цільової аудиторії людей або груп. В якості таких груп впливу можуть виступати відомі політичні діячі, діячі культури, відомі актори, керівники підприємств, викладачі вищих та середніх навчальних закладів і т.д. Для ефективності даного методу важлива присутність наступних факторів: довіра до представника групи впливу, його популярність, високі професійні якості, особисті гідності, високий офіційний пост (у минулому або теперішньому), його близькість з цільовою групою електорату і т.д.

Стверджуючі заяви. Метод полягає в поширенні різних тверджень, які представлені в якості факту, при цьому мається на увазі, що ці заяви самоочевидні і не вимагають доказів. Ці твердження можуть бути як достовірними, так і ні.

Сторона переможця. У даному методі експлуатується бажання людей бути на стороні переможця, аудиторія переконується в необхідності діяти так, щоб опинитися "на стороні, яка виграла", бути "як всі". У виборчих кампаніях метод часто використовується у вигляді наступних пропагандистських тем: "Кандидат N - кандидат номер один" або "Кандидат N - кандидат переможець", а також в закріпленні теми "Все одно переможе N".

Використання ціннісних слів (що відносяться до основних цінностей суспільства). Метод полягає у використанні емоційно інтенсивних слів, які тісно пов'язані з основними цінностями, думками суспільства і є переконливими без додаткової інформації та зв'язуванні їх з необхідними ідеями або людьми. Даний метод апелює до таких почуттів як любов до країни, дому, бажання миру, свободи, бажання гордитися батьківщиною і т.д. Для цього використовуються слова, пов'язані з такими поняттями, як будинок, сім'я, діти, материнство, патріотизм, любов, мир, щастя, здоров'я, прогрес і т.д.

Невизначені вирази (позитивно забарвлені). Метод має багато спільного з методом "використання ціннісних слів", але заснований на використанні виразів з неуточненим смислом. Аудиторії пропонується можливість шукати власні інтерпретації. Наприклад, у виборчих кампаніях нерідко зустрічаються гасла "Я доб'юся правди (справедливості)", які, незважаючи на неясний, позбавлений "конкретики" сенс у ряді випадків сприймаються електоратом позитивно.

Найменше зло. Суть методу полягає в "м'якому" визнанні того, що певна особа або курс є неприємний, але будь-який інший призведе до результатів набагато гірших.

Спрощення проблеми. Багатьом людям не приносить задоволення довго розбиратися в тій чи іншій проблемі, а набагато зручніше отримати просту відповідь на свої питання, з іншого боку багатьом непрофесіоналам приємно почути що, наприклад, "юриспруденція це просто досвід кожної людини, заплутаний застосуванням хитрих слів", а "сучасне мистецтво - просто нісенітниця ", таким чином, люди потурають своєму почуттю переваги і побоюванню визнати, що ці області знаходяться поза їх розумінням. Суть методу "спрощення" полягає у використанні цих психологічних особливостей людини. Складні соціальні, політичні, економічні чи військові проблеми зводяться до простих інтерпретацій.

Громадське несхвалення. Використовується для створення ілюзії несхвалення тих або інших дій з боку громадської думки. Основне завдання методу - створення негативного образу того кандидата або групи. Часто реалізується шляхом підбору різних висловлювань "груп впливу", "представників" різних верств населення, різних соціологічних опитувань і т.д.

Невизначені вирази і натяки, що несуть негативне забарвлення. При використанні даного методу аудиторії пропонується можливість самій знаходити власні інтерпретації. Використовується проти окремих людей, груп, ідей і експлуатує суспільні стереотипи і латентні підозри. Часто використовується у формі наступних натяків: "Ну, ви розумієте, на що зазвичай живуть такі чиновники як N".

Ігнорування. Полягає в ігноруванні елементів і тем іншої сторони, заснований на тому припущенні, що негативна тема, що залишається "на слуху" приносить більший збиток, порівняно з темою, що з'явилася на короткий проміжок часу. Найбільш ефективний у разі незначності теми, невеликих ресурсів іншої сторони для її "розкручування", а також у разі високої достовірності негативної інформації.

Висновок. У сучасному суспільстві інформація відіграє велику роль. Сьогодні за допомогою інформації можна домогтися практично будь-яких цілей. З'явилися нові підходи до застосування інформації, визначення її ролі і місця в суспільстві. З цих підходів з'явилася інформаційна війна.

Інформаційна війна явище не нове. Витоки подібних воєн можна розгледіти ще в давнину, але активно використовуватися технології інформаційних війн почали тільки в 20 столітті. Це поштовх, пов'язаний з появою комп'ютерів і бурхливим розвитком засобів масової комунікації, без яких неможливо вести ефективну інформаційну війну.

Метою інформаційної війни є введення в оману противника або підпорядкування цільової аудиторії на свою сторону, тому необхідне вирішення даної проблеми, тим більш у наш час інформація розповсюджується дуже швидко завдяки мережі Інтернет. Ця проблема ще вивчається і необхідно якнайшвидше знайти підходи, щоб з нею боротися.

Список літератури

1. Вепрінцев В. Б., Манойло А. В., Петренко А. І., Фролов Д. Б., 2003 р.: Операції інформаційно-психологічної війни: методи, засоби, технології, короткий енциклопедичний словник - М.: Гаряча лінія - Телеком, 450 с.

2.Доценко Е. Л. Психология манипуляции. Феномены, механизмы, защита. - М., 1996

3. Почепцов Г. Г. Психологические войны. - Москва - Киев: "Рефл-бук", 2000

УДК 004.056

Метод активного захисту комп’ютерних систем та мереж у ході інформаційної війни

Хох В.Д., студент 5 курсу

Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент

Кіровоградський національний технічний університет, м. Кіровоград

У сучасному світі інформація має велику ціну. Іноді це ціна великої кількості грошей, іноді це ціна людських життів а іноді ціна інформації може стати приводом для відкритого дипломатичного конфлікту між державами, наприклад атака на Sony Pictures Entertainment, що, майже призвела до повернення Північної Кореї до списку країн що підтримують тероризм, а компанія втратила приблизно 130 мільйонів доларів США. Надання спотвореної або заздалегідь невірної інформації призводило і до геноциду цілих народів, один з

прикладів – геноцид народності Тутсі в Руанді (1994 р.), ця подія дала змогу доценту економісту з Гарварду – Девіду Янагідзава-Дротту (David Yanagizava-Drott) виявити чітку емпіричну залежність між поширенням інформації, у даному випадку поширення небезпечної інформації відбувалося завдяки радіо, та кількістю вбитих людей [1]. Отже стає все більш помітним той факт що інформація це дуже ефективний інструмент та цінний ресурс.

У 1996 р. корпорація «RAND» опублікувала звіт MR-661-0SD – «Стратегічна інформаційна війна (або спротив)» (в оригіналі «Strategic Information Warfare») [2]. В ньому було дане визначення ***інформаційної війни*** (ІВ) як війни з використанням державного глобального інформаційного простору й інфраструктури для проведення стратегічних військових операцій і зміцнення впливу на власний інформаційний ресурс. Тобто вже у 1996 р. інформаційну війну сприймали як різновид агресії або впливу на супротивника під час проведення збройних операцій. У цьому ж звіті були перераховані деякі переваги ІВ, наприклад, розмитість традиційних кордонів між злочинною та військовою (оригінал «warlike») діяльністю. Це можна побачити на сході України, коли після загибелі великої кількості кадрових російських військових їх їхня держава визнає або заблукавшими або ополченцями.

У цьому ж звіті [2] розкриті основні властивості стратегічної інформаційної війни, до них входять:

- Низька вартість «входу» - на відміну від традиційних воєнних технологій – інформаційні потребують значно менших фінансових або інших матеріальних вкладень, як для розробки так і застосування.
- Розмиті традиційні кордони – кордони між інтересами масовими та особистими, поведінкові кордони між злочинною та військовою (оригінал «warlike») діяльністю. А також між географічними кордонами таких націй де історично склалося так, що інформаційні структури вплетені одна в одну.
- Розширена роль управління сприйняттям – нові інформаційно-орієнтовні техніки дозволяють суттєво збільшити потужність обману та маніпуляцій, що драматично відобразиться на політично-суспільних ініціативах, спрямованих на підтримку оборонної діяльності.

В [2] також відзначається складність проведення аналізу та збору розвідданих щодо нанесення нових ударів, немає чіткого поля аналізу та стратегій визначення можливих ударів.

Ще один, нині поширений термін – ***кібервійна***. Український професор Мережко О.О. [3] визначає кібервійну як використання Інтернету та пов'язаних з ним технологічних і інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній безпеці та суверенітету іншої держави. Дане визначення не дає чіткої відповіді на те, як використовуються і які саме технології застосовуються для заподіяння шкоди. Це важливо, оскільки багато людей, і все більше, не використовують або не довіряють інформації з телевізору або радіо і використовують мережу Інтернет для отримання необхідної інформації. Маніпулювання такою інформацією також шкодить державі, проти якої ведеться агресія, але це підпадає під означення ІВ. Тут необхідно згадати угрупування Anonymous, яке задля досягнення своїх цілей використовувало Інтернет технології як для викрадення та поширення певної інформації, так і для саботування систем. І цілей, у більшості випадків, вони досягали. Anonymous не використовували ЗМІ, але своїми діями привертали їх увагу та впливали на сприйняття глядача. Для визначення кібервійни дуже важливо чітко визначити, що буде саме її проявом, а що буде проявом ІВ, оскільки кордон між ними досить розмитий. І можливо це стало причиною появи іншого терміну – ***iWar*** що було введено НАТО у 2008р під час нападу Росії на Грузію.

Термін iWar не має чіткого означення, його було застосовано для того щоб

охарактеризувати діяльність спецслужб Росії в інформаційному середовищі як Грузії так і самої Росії. Тоді було виведено з ладу багато сайтів уряду Грузії, на них були розміщені фотографії Гітлера, заклики до координації та спрямування діяльності проти Грузії у мережі Інтернет, у той же момент російські телевізійні канали запустили марафон з освітлення військової агресії своєї країни, пояснюючи її «примушенням Грузії до миру». За рік до цих подій атаки зазнала Естонія, під час загострення відносин з Росією, через перенос пам'ятника Бронзовому солдату у Таллінні. Від цієї атаки постраждали та були виведені з ладу сайти парламенту Естонії, банківських установ, ЗМІ та міністерств. Естонських спеціалістів, що були задіяні під час тих подій, було відряджено до Грузії для допомоги у вирішенні проблем, пов'язаних з діями агресора.

Враховуючи вищесказане, можна сказати, що кібервійна та інформаційна війна є складовими iWar, оскільки даним терміном охарактеризовано комплексну діяльність певної країни у інформаційному просторі як своєму так і в країні – жертві агресії. З використанням як Інтернет технологій так і ЗМІ. До того ж Інтернет технології застосовувались не лише для поширення та маніпуляції інформацією а й для виведення з ладу серверів країни, що зазнала агресії. Держава має бути захищеною від такої агресії, а вразі якщо агресія вже відбувається – повинна мати можливість активно захищати себе.

iWar, безумовно, ефективна тактика. І, безумовно, це невід'ємна складова традиційного збройного конфлікту в сучасному світі.

До пасивного захисту від iWar відноситься:

- Використання брандмауерів для збереження цілісності периметру системи або мережі, що підлягає захисту.
- Виявлення та знешкодження небезпечного програмного забезпечення і шпигунського ПЗ.
- Виявлення та адекватне реагування на фізичні засоби стеження (напр., закладки).
- Ефективна протидія засобам дистанційної технічної розвідки.
- Якісне та ефективне застосування засобів криптографії та стеганографії.
- Ефективне проведення політики безпеки серед персоналу або окремо взятої особи, що працює з системою або мережею, що підлягає захисту.

До активного захисту від iWar можна віднести наступне:

- Попереджувальна перевірка систем або мереж, що тим чи іншим чином пов'язані з системою або мережею, що підлягає захисту.
- Виявлення та знешкодження потенційно небезпечних систем або встановлення нагляду за такими системами або мережами.
- Ефективне виявлення джерела атаки та його знешкодження.
- Збір інформації про супротивника.
- Знешкодження стратегічних вузлів супротивника.

Активний захист комп'ютерної мережі або системи полягає у знешкодженні обладнання, яке може бути застосоване для координації дій агресора або проведенні кібератаки. Також, використовуючи методи активного захисту, стає можливим отримання інформації про координацію збройних сил супротивника або саботаж збройних операцій завдяки втручанню у механізми передачі інформації.

Розглянемо ситуацію коли виявлено систему, яка потенційно може бути використана для організації кібератаки. Задача полягає в унеможливлені несподіваної атаки з цієї системи. Оскільки особистість власника цієї системи визначити відразу не вдається, стає неможливо визначити його причетність до сил агресора. Також неможливо фізично дістатися системи та визначити причини її підозрілої активності, якщо ж активність цієї системи чітко розпізнана як підготовча діяльність до атаки або невдала атака, необхідно вдатися до активних дій і встановити стеження за цією системою за допомогою спеціального програмного забезпечення (СПЗ). Через неможливість фізично дістатися системи необхідно розгорнути СПЗ віддалено. Першим етапом буде збір усієї можливої інформації про систему

супротивника та її аналіз. Для збору такої інформації застосовують сканери портів, різноманітні сніфери та деякі специфічні тести. Хоча застосування такого ПЗ і не викликає помітних змін у роботі системи воно може і часто залишає багато слідів у log`ах обладнання та програмного забезпечення досліджуємої системи.

В даній роботі запропоновано метод активного захисту комп'ютерних систем та мереж в ході інформаційної війни.

У запропонованому методі, для того щоб запобігти виявленню на стадії збору інформації за умови дефіциту часу, пропонується використовувати віддалені системи, які не пов'язанні між собою географічно. В системах, що використовуються для збору інформації, пропонується встановити автоматизовані агенти, між якими буде відбуватися розподілення завдань по скануванню та проведенню тестів на досліджуваній системі. Таким чином, навіть якщо в мережі або системі, що досліджується, ведуться log`и, їх буде достатньо зашумовано, для того щоб не було можливості виявити, а відтак і заблокувати координатора дослідження. Розподілення сканування також має на меті ускладнити процес аналізу log`ів та показань сніферів на стороні досліджуємої системи, якщо такі застосовуються. Зібрана інформація має концентруватися на тимчасовому сервері, а згодом передаватися на головний сервер, де буде проходити її аналіз. Після проведення аналізу визначається список або списки СПЗ, яке відповідає поточним потребам того, хто проводить операцію, та є сумісним з тими вимогами, що були висунуті під час аналізу зібраної інформації. Наступним кроком є застосування СПЗ та його розгортання в системі супротивника. Один з методів, що застосовується на даному етапі це "Heil Mery", він полягає у тому, що до ворожої системи застосовується одне за одним СПЗ зі списку. Такий метод не лише залишає дуже помітні сліди у log`ах, але й може викликати збій у роботі системи, що з великою вірогідністю викличе підозри. Однак, застосувавши той же принцип розподілення задач між віддаленими системами з автоматизованими агентами, є можливість знизити ризик викликати збій у роботі системи, і, навіть, якщо один з вузлів викличе підозру і буде заблоковано, це не призведе до зупинки усього процесу. Після того як буде виконана побудова списку, необхідно підготувати СПЗ та завантажити його на сервер, з якого автоматизовані агенти завантажать його на свої системи та за командою почнуть застосовувати його до системи супротивника. У супротивника не буде змоги заблокувати систему до того як вона застосує свою частину СПЗ зі списку, так як йому невідомо коли і з якої системи це відбудеться, а оскільки СПЗ, що було застосовано за допомогою автоматизованого агента буде намагатися зв'язатися не з системою, з якої була запущена то блокування системи з агентом ніяк не відобразиться на успішності проведення операції.

Чіткої протидії від таких операцій немає і не може бути, оскільки у випадку якщо в операції приймали участь достатньо кваліфіковані спеціалісти передбачити їх дії на етапі побудови списку СПЗ неможливо. Серед СПЗ може бути таке, що було розроблено спеціально для системи, яка є ціллю операції, а тому може відпасти необхідність в застосуванні всього спектру СПЗ зі списку. Однак ускладнити проведення такої операції можливо, одним з найбільш дієвих способів є регулярне оновлення ПЗ на системі, що підлягає захисту. Також класичні рішення такі як антивіруси можуть зреагувати на багато СПЗ, якщо спеціалісти не вдалися до запобіжних заходів, але якщо вдалися - ефективність антивірусів значно знижується. Добре налагоджений брандмауер може стати порятунком, оскільки може запобігти збору інформації, а отже заблокувати роботу ще на стадії її підготовки. Успішне проведення операцій активного захисту дає змогу розгорнути на ворожих системах СПЗ з великим спектром можливостей – збір інформації, маніпуляція інформацією, втручання в механізми передачі інформації, виведення з ладу вузлів зв'язку та багато іншого. Одна з привабливих функцій – це здатність до розповсюдження, що може дати змогу слідкувати відразу за багатьма учасниками агресії, єдине зауваження це те, що таке розповсюдження важко контролювати, а отже рано чи пізно це СПЗ буде помічено та піддано аналізу, що може призвести до усунення джерел розгортання та діяльності цього

СПЗ і доведеться проводити операцію знову.

В сучасному світі інформація це багатофункціональний інструмент та цінний ресурс. Проведення політики активного захисту в ході інформаційної війни дає змогу отримати важливу та своєчасну інформацію, а також деморалізувати супротивника.

Список літератури

1. David Yanagizawa-Drott Propaganda and Conflict: Evidence from the Rwandan Genocide - 10.2014 Quarterly Journal of Economics 129(4) [Електронний ресурс] – Режим доступу: http://www.hks.harvard.edu/fs/dyanagi/Research/RwandaDYD.pdf

2. Roger C. Molander, Andrew Riddile, Peter A. Wilson Strategic Information Warfare: A New Face of War – Monograph report MR-661 [Електронний ресурс] – Режим доступу: http://www.rand.org/pubs/monograph_reports/MR661.html

3. Мережко О.О. Проблеми кібервійни та кібербезпеки в міжнародному праві - 05.09.2009 для Українського центра політичного менеджменту [Електронний ресурс] – Режим доступу: http://www.justinian.com.ua/article.php?id=3233

УДК 004.056

Дослідження методів психологічної війни

Цимбал Є.В., студент 3 курсу
Науковий керівник – Константинова Л.В., викладач
Кіровоградський національний технічний університет, м. Кіровоград

Поняття «психологічна війна» стає все більш популярним. Воно використовується не тільки в наукових працях, а й у художніх фільмах. Поява кіноплівок і виступів різних громадських діячів, які стверджують наявність інформаційних атак і маніпуляцій свідомістю, дозволяє констатувати актуальність вивчення методів психологічних війн.

Психологічна війна в такому вигляді існує стільки часу, скільки існує сама людина. Проте в далекому минулому люди вміли впливати один на одного тільки в процесі безпосереднього спілкування, надаючи вплив на своїх співрозмовників за допомогою слів, інтонації, жестів, міміки.

Сьогодні способи впливу на людську свідомість стали набагато різноманітнішими, дієвими і витонченими завдяки накопиченому за тисячоліття практичному досвіду, а також за рахунок створення спеціальних технологій спілкування, взаємодії та управління людьми.

Психологічна війна – сукупність різних форм, методів і засобів впливу на людину з ціллю зміни в бажаному напрямку її психологічних характеристик (поглядів, думок, настроїв, установок, мотивів, стереотипів поведінки), а також групових норм, масових настроїв, суспільної свідомості в цілому.

Цей термін тісно пов'язаний з терміном психологічна операція. Оскільки психологічна війна ведеться за допомогою інформації, її варто розглядати як вид інформаційної війни.

Вперше поняття «психологічна війна» використав доктор М. Кампанео у своїй книжці «Досвід військової психології».

Сьогодні політика «психологічної війни» є окремим напрямком діяльності більшості країн. Характерними рисами сучасної психологічної війни є [1]:

- *глобальність* - вплив на всі сфери життєдіяльності супротивника, нейтральних держав, союзників, свого населення і збройних сил;

- *тотальність* - проникання в усі сфери життя: в дипломатію, економіку, культуру, суспільні стосунки, соціально-психологічну тощо;

- *технізація* - широке використання досягнень науки й техніки як для опрацювання змісту, методів і прийомів психологічної війни, так і форм та способів їх реалізації;

- *організованість* - створення різноманітних органів психологічної війни та чітка координація їхніх зусиль і напрямів діяльності (у всіх розвинених країнах вони об'єднані в єдину державну структуру).

Методами психологічної війни можна вважати:

- пропаганда;
- дезінформація;
- провокації;
- саботаж;
- терор;
- поширення пліток;
- створення паніки;
- випуск фальшивих грошей, документів тощо.

Пропаганда – форма комунікації, спрямована на поширення фактів, аргументів, чуток та інших відомостей для впливу на суспільну думку на користь певної спільної справи чи громадської позиції. Пропаганда зазвичай повторюється та розповсюджується через різні засоби масової інформації, щоб сформувати обраний результат суспільної думки.

Дезінформування або *дезінформація* – спосіб психологічного впливу, що полягає в намірі подання об'єктові такої інформації, яка вводить його в оману відносно справжнього стану справ та створює викривлену реальність. Поширення перекручених, неповних або свідомо неправдивих відомостей для досягнення пропагандистських, військових (введення противника в оману), комерційних або інших цілей.

Провокація – дія або низка дій, які мають на меті викликати реакцію тих, кого провокують. Як правило, проводяться, з метою штучного створення складних обставин або негативних наслідків для тих, кого провокують. Суб'єкт, що здійснює провокації, називається провокатором. Оскільки провокації ґрунтуються на особливостях психології людини, її поведінці як соціальної істоти, вони вивчаються психологією та соціологією.

Саботаж - це навмисний зрив роботи чи якогось заходу шляхом прямої відмови від нього, прямої протидії його виконанню, свідомо недбалого її виконання або формального безініціативного виконання з дотриманням лише видимості виконання; одна з форм економічної боротьби працівників проти підприємців.

Терор – насилля представників влади з використанням державного апарату проти народу з метою придушення не тільки опозиції, але й всього загалу, з метою викликати жах і залишити думки про опір. Іншими словами, терор – насилля з боку наділеного владними повноваженнями ("сильніших").

Плітки – особлива, зазвичай недостовірна інформація (яка спотворює інформацію), що розповсюджується виключно в усній формі, як би «по секрету», «з вуст у вуста», і функціонуюча виключно в звуковій формі.

Паніка – психічний стан людей - несвідомий, нестримний страх, викликаний дійсною чи уявною небезпекою, що охоплює людину чи багатьох людей, неконтрольоване прагнення уникнути небезпечної ситуації.

Фальшиві гроші, документи – гроші та документи, що створені з порушенням встановлених законодавством норм і містить неправдиві відомості про людину, фірму чи інші дані.

Цілями психологічної війни є: вплив на почуття, волю, емоції, свідомість і підсвідомість, мотиваційну сферу з метою деморалізації супротивника, підриву його власних поглядів, ціннісних орієнтацій, переконань і нав'язування йому своїх ідей.

Отже, із визначень психологічної війни випливає наступне [8]:

1. Психологічна війна полягає у використанні не тільки пропаганди, а й багатьох інших заходів. У психологічній війні допускаються всілякі засоби заради досягнення поставлених цілей: отруєння продовольства, знищення великих індустріальних об'єктів, вбивства, терор, саботаж та інші, які вважаються цілком придатними для досягнення своїх цілей. Підрив морального стану ворога - ось головна мета, досягти яку намагаються веденням психологічної війни.

2. Психологічна війна ведеться не тільки у воєнний час. Це особливий вид підготовки та проведення війни, який ведуть постійно. Недарма в американському «Посібнику з ведення психологічної війни» вказується, що «Психологічна війна ... не знає жодних кордонів між війною і миром. Вона ведеться постійно, тобто як в мирний, так і у воєнний час». Ведення психологічної війни в мирний час - це саме та діяльність, яка відома під назвою «холодна війна» [4].

3. Психологічна війна ведеться правлячими колами як проти свого народу, так і проти народів ворожих держав, а також проти народів нейтральних і дружніх країн. Досвід першої та другої світових воїн підтверджує це. [5].

4. Метою психологічної війни є підготовка та ведення агресивних воїн в політико-ідеологічному, моральному і психологічному аспектах. Все це робиться насамперед для того, щоб вплинути на почуття людей, викликати панічний страх, порушити у народу ненависть до інших народів, зіграти на цих людських почуттях. Все це правлячі кола роблять для того, щоб перетворити людей на слухняне знаряддя для здійснення своїх військових планів. Узагальнивши все сказане, можна сформулювати наступне.[6]

Психологічна війна - це особливий вид підготовки і ведення воєн, що дозволяє панівним колам, використовуючи пропаганду, терор та інші засоби, впливати на власні народи, народи ворожих, союзницьких і нейтральних країн у політико-ідеологічному, моральному і психологічному аспектах для досягнення цілей своєї військової стратегії.[2]

Психологічну війну можна визначити як планомірне використання державою та її установами засобів і заходів ідеологічної дезорієнтації та розкладання свідомості людей і груп людей з метою зниження їхньої ідейної, політичної, духовної та морально-психічної стійкості, спонукання до негативних дій або бездіяльності населення та особового складу армій інших держав як у воєнний, так і в мирний час.

Отже, необхідно знати методи психологічної війни для захисту себе від шкідливого впливу невірної інформації, бо як кажуть: "Хто володіє інформацією, той володіє світом".

Список літератури

1. Морозов. А. Психологическая война. Киев, 1996.
2. Лайнбарджер П. Психологическая война - М.: Воениздат, 1962. - 350 с.
3. Репко С.И. Отечественный опыт ведения спецпропаганды (1918-1991). М.: Воен. ун-т, 1994. – 620с
4. Севрюгин В.И. Специальные методы социально-психологического воздействия и влияния на людей. - Челябинск: Обл. ид-во, 1996. - 416 с.
5. Техника дезинформации и обмана/Под ред. Я. Н. Засурского. - М.: Мысль, 1978. - 248 http://bookap.info/psywar/krysko/gl15.shtm
6. W. Daugherty and M Jannowitz, A Psychological Warfare Casebook, The John Hopkins Press, Baltimore, 1958.
7. Крысько В.Г. Секреты психологической войны. (цели, задачи, методы, формы, опыт). Издательство: Минск 1999.
8. Синякова В.Б. Психологічна війна [Електронний ресурс] – режим доступу: http://kyiv-oblosvita.gov.ua/images/banners/17_03_2014/pcugolog_viuna.doc

УДК 004.056.53

Огляд способів застосування глобальної комп'ютерної мережі Інтернет в інтересах інформаційного протиборства

Цимбал Н.О., студентка 3 курсу
Науковий керівник – Гермак В.С., викладач
Кіровоградський національний технічний університет, м. Кіровоград

В даний час Інтернет все активніше і масштабніше використовується в інтересах інформаційного протиборства сторін, які є учасниками різних конфліктів. Він надає широкі можливості для створення впливу на формування громадської думки, прийняття політичних, економічних і військових рішень, впливу на інформаційні ресурси противника і поширення спеціально підготовленої інформації (дезінформації). Активне використання мережі Інтернет для ведення інформаційного протиборства обумовлено наявністю низки її істотних переваг перед звичайними засобами і технологіями передачі інформації.

1. Оперативність. Розміщення і регулярне оновлення інформації на окремих сторінках, в інтернет-виданнях і різного роду розсилках новин, форумах і конференціях не вимагають значного часу на підготовку матеріалів в електронному вигляді. При цьому користувачі отримують її в режимі реального часу (на відміну, наприклад, від читачів періодичних видань). Крім того, цілеспрямований вплив на інформаційні ресурси противника може здійснюватися не тільки в заздалегідь запланований час, але і по мірі виникнення необхідності.

2. Економічність. Є наслідком залучення невеликої кількості персоналу і матеріальних засобів для вирішення поставлених задач. Так, нерідко буває цілком достатньо наявності мінімально підготовленого користувача персональної ЕОМ, підключеної до телефонної лінії. Крім того, застосування комп'ютерних технологій для виведення з ладу систем управління протилежної сторони в певних умовах може призвести до більш значного ефекту при значно менших витратах в порівнянні з використанням традиційних засобів.

3. Скритність джерела впливу. Як правило, акт агресії в глобальній мережі важко відрізнити від дії звичайних комп'ютерних хуліганів. Підготувати та провести кібератаку з використанням Інтернету може досить широке коло осіб - від військових і розвідувальних структур іноземних держав до партизанських формувань, хакерів або просто озлоблених людей. Відстежити ж джерело досить складно.

4. Дистанційний характер впливу на комп'ютерні системи в різних регіонах світу. В оглядах порушень мережевої безпеки регулярно повідомляється про виявлені наслідки ефективних дистанційних впливів на комп'ютерні мережі різних країн.

5. Масштабність можливих наслідків. Крім впливу на формування громадської думки, на позиції офіційних осіб, які приймають найважливіші рішення, використання глобальної мережі для деструктивних впливів може призвести до порушення нормальної роботи життєво-важливих об’єктів і систем.

6. Комплексність подачі інформації та її сприйняття. На Інтернет-сторінках розміщується як текстова, так і графічна інформація в найбільш зручному для сприйняття вигляді, а її обсяг може бути в багато разів більше, ніж у будь-якого друкованого видання, радіопередачі або телевізійної програми. Використання ж сучасних мультимедійних технологій, що дозволяють демонструвати документальні свідчення, фото- та відеоматеріали при спеціально підібраному супроводі (коментарі, музика), створює на користувачів

додатковий емоційний вплив.

7. Доступність інформації. За наявними даними, загальна кількість користувачів Інтернету в 2014 році досягла 3 мільярдів. Миттєво вони отримують доступ до інформації, наявної на серверах різних країн, минаючи прикордонні, цензурні та інші бар'єри. При цьому будь-який користувач може розмістити власну інформацію (нерідко безкоштовно) на серверах, зареєстрованих в інших державах, або організувати розсилання повідомлень по всьому світу.

Розглянемо деякі напрями використання глобальної комп'ютерної мережі Інтернет в інтересах інформаційного протиборства.

1. Поширення спеціально підібраної інформації (дезінформації). Воно здійснюється шляхом: розсилки електронних листів e-mail; організації груп новин; створення сайтів для обміну думками; розміщення інформації на окремих сторінках або в електронних версіях періодичних видань та мережного мовлення (трансляції передач радіо- і телестанцій). Найбільш поширеним напрямком використання глобальної мережі в інтересах вищезгаданого протиборства є заміна інформаційного змісту сайтів, що полягає в підміні сторінок або їх окремих елементів в результаті злому. Такі дії робляться в основному для залучення уваги до атакуючої сторони, демонстрації своїх можливостей або є способом вираження певної політичної позиції. Особливо слід виділити так звані семантичні атаки, які полягають у зломі сторінок і наступному акуратному (без помітних слідів злому) розміщенні на них завідомо неправдивої інформації. Подібним атакам, як правило, піддаються найбільш часто відвідувані інформаційні сторінки, змісту яких користувачі повністю довіряють.

2. Ще одним напрямком використання Інтернету в інтересах інформаційного протиборства є виведення з ладу або зниження ефективності функціонування структурних елементів мережі. Найбільш часто вживаними способами зниження ефективності функціонування її окремих елементів є наступні:

- «Бомбардування» мережі електронними листами. Даний спосіб вважається однією з форм «віртуальної блокади», оскільки відправка великої кількості електронних послань на одну адресу протягом короткого часу ускладнює або унеможливлює отримання (виділення) адресатом «легальних» листів із загального їх масиву, а іноді може призвести і до порушення роботи обслуговуючих серверів;
- DOS-атаки, проведення яких по суті аналогічно технології масової розсилки електронних листів одному адресату і полягає в генерації величезного числа звернень до вибраного сайту. Це призводить до уповільнення роботи обслуговуючого сервера або повного припинення зовнішнього доступу до нього;
- Впровадження комп'ютерних вірусів. В інформаційному протиборстві в мережі використовуються всілякі способи впровадження різних видів вірусів та їх модифікації.

Таким чином, розвиток глобальної мережі Інтернет супроводжується все більш широким використанням наданих нею можливостей для здійснення інформаційного протиборства, зростанням координації, масштабів та складності дій її учасників, в якості яких виступають як держави або їх коаліції, так і окремі організовані групи, у тому числі терористичні. Об'єктом Інтернет-атак все частіше стають інформаційні ресурси, виведення з ладу яких може завдати протилежній стороні значних економічних збитків або викликати великий суспільний резонанс.

Список літератури.

3. Фролов Д. Б., Воронцова Л. В. Информационное противоборство: история и современное состояние – Телеком, 2003.

4. Манойло А. В. Государственная информационная политика в особых условиях, монография – МИФИ, 2003. - 388 с.

5. Прохожев А. А., Турко Н. И. Основы информационной войны, 1995.

Напрямок 10.
Електронний уряд та інші соціальні інформаційні ресурси з погляду безпеки інформації

УДК 004.42

Автоматизація функціонування Вчених рад структурних підрозділів навчально-наукових установ за допомогою програмно-апаратного комплексу «Вчена рада факультету» з використанням захищеного каналу передачі шифрованих даних

Єршов В.В., студент 6 курсу
Науковий керівник – Буй Д.Б., д-р фіз.-мат. наук, професор
Кіровоградський державний педагогічний університет імені Володимира Винниченка, м. Кіровоград

У наш час актуальним є процес автоматизації та комп'ютеризації систем, які використовуються в побуті, виробництві, навчанні. Так, зокрема, у навчальній сфері мають місце заходи з інтерактивним залученням певної кількості осіб-учасників (членів). Одним із типів структур, в якій відбуваються подібні заходи, є Вчені ради навчально-освітніх установ.

Вчена рада - постійно діючий виборний представницький орган вищого навчального закладу (ВНЗ), науково-дослідницької організації або об'єднання вчених, що займається вирішенням стратегічних питань розвитку ВНЗ, організації, території, на якій він представлений. Формування Вченої ради для державних вищих навчальних закладів є обов'язковим. До складу Вченої ради входять ректор, який є її головою, проректори, президент (якщо така посада передбачена статутом), а також за рішенням ради - декани факультетів. Інші члени ради обираються таємним голосуванням на загальних зборах (конференції), яке також визначає і загальна кількість членів ради. Норми представництва в Вченій раді від структурних підрозділів та учнів (студентів та аспірантів) визначаються Вченою радою. Звичайно загальні збори відповідних підрозділів висувають завідуючих кафедрами, провідних вчених, керівників служб забезпечення, членів студентського активу. Представники структурних підрозділів вважаються обраними до складу Вченої ради або відкликаними з нього, якщо за них проголосували більше двох третин делегатів, присутніх на загальних зборах (за наявності не менше двох третин спискового складу делегатів). Склад Вченої ради вищого навчального закладу оголошується наказом ректора. У разі звільнення (відрахування) члена Вченої ради він автоматично вибуває з її складу. Термін повноважень Вченої ради не може перевищувати 5 років. Дострокові вибори ради проводяться на вимогу не менше половини його членів, а також у випадках, передбачених статутом вищого навчального закладу. Так, можна розглянути процес голосування у Вченій раді вищого

навчального закладу, коли члени зібрання голосують за ухвалення певного рішення, винесеного на порядок денний.

Мета проекту полягає в забезпеченні автоматизації процесу голосування під час засідань Вчених рад шляхом використання портативних (мобільних) пристроїв – смартфонів, планшетів – сьогодні доступних кожному з членів ради. Перевагами застосування даної системи є економія ресурсів (енергетичних, витратних) часу, необхідного на процедуру проведення голосування, протоколювання та збереження результатів голосування базах даних (електронний документообіг) з можливістю звернення до них та подальшого використання, мінімізація зусиль, витрачених на підготовку до проведення голосування (секретарю пропонується керувати перебігом голосування з персонального комп'ютера), мінімізація людського фактору, низька собівартість використання комплексу. За допомогою сучасних інформаційних технологій планується підвищити ефективність діяльності Вчених рад всіх рівнів (факультет/інститут, університет/інститут/академія), зокрема, спеціалізованих Вчених рад науково-навчальних установ.

Для реалізації поставленої мети виконано такі завдання:

- розробка мобільної програмно-апаратної системи електронного голосування, яка не потребує спеціального приміщення для монтажу стаціонарного обладнання та може бути розгорнута в прийнятний час;
- уніфікація документації, зокрема, автоматична підготовка бюлетенів для голосування, протоколів лічильних комісій, різноманітних звітів, довідок та витягів з протоколів засідань;
- автоматизація контролю виконання рішень, накопичення інформації в базі даних для її наступного аналізу.

Створений комплекс автоматизації функціонування Вчених рад структурних підрозділів науково-навчальних установ на сьогодні не має аналогів на теренах нашої держави та поза її межами. Планується його апробація та подальше впровадження у роботу в межах різноманітних структурних підрозділів Вчених рад (на рівні, факультету, вищого навчального закладу). Комплекс потенційно може бути застосований для проведення голосування у міських, селищних, районних радах (з огляду на низьку собівартість та зручність експлуатації).

Під час виконання дослідження розроблено багатокомпонентний програмний комплекс, який забезпечує автоматизацію функціонування Вчених рад. Розробка комплексу являє системний підхід до дослідження усіх аспектів реалізації компонентів пристрою. Одним з ключових аспектів є розробка мобільного додатку, який реалізує отримання/передачу даних мережею, створеного за допомогою середовища розробки Xcode.

Клієнтський додаток забезпечує взаємодію члена Вченої ради з секретарем Вченої ради шляхом отримання та пересилання інформації на сервер та встановлюється на пристрої iPhone, iPad, iPod Touch, які є власністю члена Вченої ради. В подальшому передбачається розробка аналогічних додатків для інших поширених мобільних платформ – Android та Windows Phone.

Сервер реалізовано за допомогою середовища розробки Microsoft Visual Studio 2010 для операційних систем Windows.

Серверний додаток забезпечує проведення голосування в рамках засідання Вченої ради шляхом надсилання питань, які виносяться на голосування, на бездротові пристрої членів ради, отримання відповіді від них та працює під управлінням операційної системи Microsoft Windows, зважаючи на поширеність використання даної системи у відповідних установах.

У реалізованому програмно-апаратному комплексі забезпечено кількарівневий захист користувацьких даних. Зокрема, використовуваний протокол з'єднання не допускає під час сесії проникнення до каналу сторонніх даних від жодного іншого джерела, окрім клієнта та сервера. Крім того, у програмному алгоритмі системи передбачена аутентифікація

користувача, що забезпечує унікальність голосу кожного члена Вченої ради. Це дає змогу усунути недолік архітектури систем даного типу (наприклад, електронної системи «Рада», що використовується у сесійній залі Верховної Ради України) - неможливість фізичного забезпечення унікальності голосу конкретної особи (явище, відоме як «кнопкодавство»). Авторизаційні відомості користувача з міркувань захисту даних та анонімізації шифровані на стороні клієнта з використанням MD5 сум і вже в шифрованому вигляді надходять на сервер. З тих же міркувань безпеки у базі даних сервера усі дані про користувачів і здійснені ними голоси зберігаються у шифрованому вигляді.

Науково-технічна продукція складається з дистрибутива програмно-апаратного комплексу (інсталяційного програмного забезпечення) та низки інструкцій користувача: інструкція з інсталяції комплексу, інструкція з адміністрування комплексу, інструкцій користувачів комплексу «Голова Вченої ради», «Вчений секретар Вченої ради», «Користувач» (всі користувачі розподіляються за функціями, які вони можуть виконувати; так голова може формувати порядок денний, оголошувати реєстрацію членів ради, проводити голосування, а рядовий член ради – реєструватися та голосувати; звичайний користувач може тільки переглядати відповідну інформацію).

Висновки. Розроблено апаратно-програмний комплекс, призначений для забезпечення функціонування Вчених рад структурних підрозділів науково-навчальних установ, до складу якого входять такі компоненти: керуючий сервер (користувач – голова зібрання або секретар Вченої ради), програмний додаток для мобільного пристрою (користувач – член Вченої ради, на пристрій якого встановлено додаток), додаток для персонального комп'ютера (зокрема, ноутбука), в разі, якщо відсутній доступ до мобільного пристрою. В рамках реалізації серверної частини було реалізовано ряд функцій, які суттєво спрощують проведення засідань Вченої ради, зокрема формування з подальшим експортом протоколу засідання в прикладне програмне забезпечення Microsoft Office Word, сповіщення заздалегідь членів Вченої ради про порядок денний через електронну пошту. Комплекс має можливість широкого застосування у практичній сфері, а також потенційну можливість адаптації до використання в інших організаціях (міських, районних, селищних радах тощо).

Список літератури

1. Бегг К. Базы данных. Проектирование, реализация и сопровождение. Теория и практика. – Вильямс, 2003. – 1436 с.
2. Братчиков И. Синтаксис языков программирования.– М. Наука, 1975.–232 с.
3. Гуц А. Математическая логика и теория алгоритмов. – Омск: Наследие, 2003. – 108 с.
4. Гэлловей М. Сила Objective-C 2.0. Эффективное программирование для iOS и OS X. – СПб.: Питер, 2014. – 304 с.
5. Далримпл М. Objective-C 2.0 и программирование для Mac. – Вильямс, 2010. – 315 с.
6. Донован Д. Системное программирование. – М.: Мир, 1975. – 540 с.
7. Здзиарски Д. iPhone SDK. Разработка приложений. – БХВ, 2012. – 506 с.
8. Керниган Б. Язык программирования С. – Вильямс, 2009. – 292 с.

НАУКОВЕ ВИДАННЯ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

“Інформаційна безпека держави, суспільства та особистості”

16 квітня 2015 року

Тези доповідей надруковано в авторській редакції.

Відповідальна за випуск: Мелешко Є.В.

Підписано до друку 15.04.2015
Тираж 70 прим.