МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«НАЦІОНАЛЬНИЙ ГІРНИЧИЙ УНІВЕРСИТЕТ»
ІНСТИТУТ ЕЛЕКТРОЕНЕРГЕТИКИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА БЕЗПЕКИ ІНФОРМАЦІЇ ТА ТЕЛЕКОМУНІКАЦІЙ

РАДА МОЛОДИХ ВЧЕНИХ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. БЕЗПЕКА ТА ЗВ'ЯЗОК

VI ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ СТУДЕНТІВ, АСПІРАНТІВ, МОЛОДИХ ВЧЕНИХ

3 квітня 2014 р.

м. Дніпропетровськ

УДК [004+621.39](06)
І 74
ББК 32.973

Оргкомітет:

Голова:	Декан факультету інформаційних технологій, д.т.н., професор Алексєєв М.О.
Заступник голови:	Голова ради молодих вчених факультету інформаційних технологій Мєшков В.І.
Члени оргкомітету:	д.т.н., професор Бабенко Т.В. д.т.н., професор Корнієнко В.І. к.ф.-м.н., доцент Гусєв О.Ю. к.т.н., доцент Галушко О.М. к.ф.-м.н., доцент Магро В.І. ст. викл. Войцех С.І. ст. викл. Тимофєєв Д.С. ст. викл. Кручінін О.В.

І 74

Інформаційні технології. Безпека та зв’язок: Матеріали всеукр. наук.-практ. конф. – Д.: Державний ВНЗ «Національний гірничий університет», 2014.– 63 с.

Викладено тези доповідей учасників VI Всеукраїнської науково-практичної конференції «Інформаційні технології. Безпека та зв’язок», яка відбулася у Державному ВНЗ «Національний гірничий університет» 3 квітня 2014 року. На конференції було розглянуті найбільш актуальні проблеми розвитку інформаційних технологій, безпеки та зв’язку в Україні та шляхи їх вирішення.

Державний ВНЗ «Національний гірничий університет»

УДК [004+621.39](06)
ББК 32.973

ЗМІСТ

Секція «Інформаційна безпека»

Секція «Інформаційно-вимірювальні технології»

Секція «Інформаційні технології»

Секція «Телекомунікації»

УДК 044.056.53

Аналіз факторів кіберзлочинства

Горошко Т.С., Масальська О.О.
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/,
E-mail: tatyanagoroshko@mail.ru

У статті аналізується кіберзлочинство на прикладі життєвого циклу шкідливого програмного забезпечення. Продемонстровані найбільш розповсюджені загрози інформації й обчислювальній техніці звичайних громадян та напрямки атаки шахраїв, а також обґрунтована неефективність існуючої боротьби з ними.

Ключові слова – небезпечне програмне забезпечення, кіберзлочинство.

ВСТУП

Незважаючи на прийняте законодавство по боротьбі з кіберзлочинністю, її склад досі чітко не описаний, як і не має загальновизнанного визначення поняття «комп'ютерна злочинність». Це обумовлено безперервним ростом можливостей технічних засобів, програмного забезпечення, засобів телекомунікацій, так і кримінальних хитрувань самих кіберзлочинців з розвитком науково-технічного прогресу і відсталістю правових норм протидії.

Кіберзлочинність можна визначити як незаконні дії, які здійснюються людьми, які використовують інформаційні технології для злочинних цілей. Серед основних видів кіберзлочинності виділяють поширення шкідливих програм, злом паролів, крадіжку номерів кредитних карт та інших банківських реквізитів, а також поширення протиправної інформації (наклепу, порнографічних матеріалів) через мережу Інтернет.

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Загроза – це потенційна можливість події, яка чинить небажаний вплив. Загроза реалізується через вразливість – слабке місце у системі захисту інформації.

У даній роботі основні загрози, що надходять з кіберпростору, а також можливі напрямки їх атак будуть розглянуті на прикладі одного з яскравих прикладів кіберзлочинності – шкідливого програмного забезпечення.

Програми з потенційно небезпечними наслідками (далі – шкідливі програми – ШП) – це окремі програми (набори інструкцій), які мають спроможність виконувати будь-яку непусту множину наступних функцій:

- приховування ознак своєї присутності в програмно-апаратному середовищі мережі;
- здатність до самодублювання, асоціювання себе з іншими програмами і (або) перенесення своїх регламентів в інші ділянки оперативної або зовнішньої пам'яті;
- руйнування (спотворення) кодів програм в оперативній пам'яті;
- збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої);
- спотворення довільним чином, блокування і (або) підміна масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті;
- придушення інформаційного обміну в телекомунікаційних мережах, фальсифікування інформації в каналах управління;
- нейтралізація роботи тестових програм і систем захисту інформаційних ресурсів.

ШЛЯХИ РОЗПОВСЮДЖЕННЯ ШП

Аналіз ринку – перша стадія життєвого циклу ШП. Він дає змогу зрозуміти, як важко буде знайти в популярних програмних продуктах вразливості, чи будуть вони цінні, чи буде вигідною покупка вразливостей у розробників або тестерів цього програмного продукту з метою використання або перепродажу.

Аналіз програмного забезпечення – другий етап життєвого циклу. На ньому проводиться детальний аналіз програмного або апаратного продукту, вибраного на першому етапі.

Розробка ШП – на даній стадії через знайдена вразливість (або кілька вразливостей) реалізується кінцевий, шкідливий продукт.

Поширення – останній етап, коли ШП інфікують пристрій, на який воно націлено. Є багато шляхів поширення шкідливих програм, у цій роботі виділимо ті, що найчастіше зустрічаються.

1. Програмна пастка представляє програмну закладку, яка використовує помилки або неоднозначність у програмному забезпеченні. Ця категорія є вразливістю сама по собі, а також може служити методом для поширення шкідливих програм, наприклад, браузером. Цей тип вразливості не новий, але він буде актуальним завжди.

2. Троянські програми – програмні закладки, які мають законний доступ до системи, проте виконують також і приховані (неоголошені) функції, тобто шкідливі програми маскуються під корисні.

3. Фішинг – спроба видати шкідливий сайт за сайт великої та відомої компанії, якій користувач довіряє. Сайт пропонує ввести свої логін та пароль, навіть дані кредитних карток, потім видає помилку і просить спробувати пізніше.

4. Спам – анонімні масові розсилки електронної пошти, найчастіше використовується для реклами товарів і послуг. Спамери наживаються на тих, хто відповідає на повідомлення. Крім того, спам слугує і для поширення шкідливих програм. Зараз поштові служби блокують більшість спам-повідомлень.

5. Бот-мережа – це мережа комп'ютерів,

заражених шкідливою програмою, яка дозволяє кіберзлочинцям віддалено керувати зараженими машинами. За допомогою бот-мережі можна організувати розповсюдження спаму, проведення DDoS-атак та розподільних обчислень.

6. Мобільні пристрої – бурхливий розвиток мобільних технологій, значне збільшення їх обчислювальних можливостей і швидкості доступу до мережі Інтернет не могли залишитися непоміченими для зловмисників. ШП для мобільних пристроїв часто крадуть персональні дані власників, відправляють дорогі повідомлення, дзвонять за кордон. Не виключені і стандартні сценарії, як відправлення спаму чи фішинг.

5. Соціальні мережі – цей спосіб стає все менш ефективним, оскільки розробники соціальних мереж покращують захист користувачів. Але і досі ШП використовують довірливість людей. Сценарії збігаються з попереднім випадком, тільки платформою для відправки повідомлень виступає клієнт обміну миттєвими повідомленнями.

6. Локальні мережі – один з найстаріших способів, але досі ефективний, що доводить недавня епідемія вірусу Conficker/Kido. Цей метод схожий на програмну пастку, але він використовує вразливості в операційних системах, мережевих протоколах, пристроях и службах.

7. Мобільні пристрої збереження інформації – усі носії від дискет до флеш-накопичувачів. Найчастіше ШП використовують автозапуск, багато хто відмовляється від цієї функції заради безпеки. Стає на заваді цьому шляху також поширення «хмарних» технологій.

ШЛЯХИ ОТРИМАННЯ МАТЕРІАЛЬНОЇ ВИГОДИ

Використовують ШП найчастіше для одержання прибутку, тобто вразливості «монетизуються» різними способами.

Зловмисник може продати вкрадену інформацію або здати в оренду обчислювальні ресурси бот-мережі. Даний тип монетизації потребує досить багато зусиль, оскільки потрібно координувати роботу великої кількості інфікованої техніки, залишаючись при цьому непоміченим.

Методи боротьби з бот-мережами на даний час неефективні, як тільки вдається припинити функціонування однієї бот-мережі, зловмисник заміняє втрачені ресурси резервними. Спіймати зловмисників майже неможливо, вони часто приховуються за довгим ланцюжком проксі-серверів. Тому потрібно приділяти значно більше уваги дослідженню кримінальних структур, що стоять за подібними порушеннями, і створити такі умови, щоб їх послуги не були потрібними.

Інший шлях – розповсюдження спаму. З цим, напевно, стикався кожен. Окрім пропозицій покупки товарів, а також фішинга, користувач може отримати і інші шахрайські повідомлення, наприклад, «нігерійські» кошти, які виманюють гроші, обіцяючи ще більше грошей.

Злодій може продати персональні дані та іншу конфіденційну інформацію – дані кредитних карт, регістраційні дані соціальних мереж, історію відвідування веб-сайтів, інформацію з пам’яті комп’ютера «жертви».

Часто зловмисники виводять зі строю обладнання і вимагають гроші за повернення працеспроможності.

ШЛЯХИ ЛЕГАЛІЗАЦІЇ

Мало заробити гроші – їх потрібно «відмити», тобто легалізувати так, щоб злочин не був виявлений. Виділяють кілька способів.

Дроп – зловмисник витрачає кошти в онлайн-магазинах, передаючи їх посередникам («дропам»), які потім повертають товар безпосередньо зловмиснику. Так не розкривається фізична адреса, навіть місто, у якому проживає зловмисник.

Оффшор – старий метод, який використовують і «класичні» злочинці. Потрібно провести суму грошей через декілька банківських рахунків так, щоб це не можна було його відстежити. Рахунки, навіть цілі банки, що беруть участь у подібних операціях, звичайно існують короткий проміжок часу, а потім безслідно зникають.

Електронні гроші – нематеріальний характер і складність відстеження операцій сприяє різним фальсифікаціям. Легко розвернути і ліквідувати.

Азартні ігри в мережі Інтернет – метод схожий на попередній, транзакції та джерело грошей дуже важко відстежити.

ВИСНОВКИ

Для боротьби з кіберзлочинством доцільно:

- вдосконалити законодавство, усунути в ньому неточності, розбіжності;
- вжити заходи по зниженню рівня хуліганської і кримінальної активності в мережі Інтернет. Можливості контролю цієї активності значно обмежено правом людей на недоторканість приватного життя;
- розробити систему з попередження шахрайств в мережі Інтернет, проведення сертифікації сайтів компаній, які проводять розрахунки між продавцем та покупцем за допомогою електронного зв’язку;
- створити сайт, що висвітлюватиме протидію вітчизняних правоохоронних органів кіберзлочинності. Цікавим прикладом слугує портал Cyber-crimes.ru, де публікуються реально розслідувані кримінальні справи.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Карпов Н., Вертузаев М. К вопросу о борьбе с компьютерными преступлениями в Украине // Закон и жизнь. – 2004. – № 7.

2. Ястребов Д.А. Институт уголовной ответственности в сфере комп. информации // Гос. и право. – 2005. – № 1.

3. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекоммуникационных сетях. — К.: МК-Пресс, 2005.

УДК 528.88

ХАРАКТЕРИСТИКА ЭКСПЕРТНЫХ МЕТОДОВ ОЦЕНКИ РИСКОВ В ПРОЦЕССЕ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Григорьева Виктория Андреевна[1], Тимофеев Дмитрий Сергеевич[2]
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, vikylya_1992@mail.ru

В данной статье рассматриваются экспертные методы оценки рисков, виды экспертных оценок и их характеристика.

Ключевые слова – риски, экспертные методы, оценка рисков управление информационной безопасностью.

ВСТУПЛЕНИЕ

Система управления информационными рисками служит фундаментом для построения системы управления информационной безопасности. Особое внимание уделяется вопросам управления, анализа и оценки рисков информационной безопасности, как необходимым составляющим комплексного подхода к обеспечению организации процесса обеспечения информационной безопасности.

Все стратегические решения по приоритезации рисков и выбору механизмов контроля необходимых ресурсов для системы управления информационной безопасности принимаются на основе результатов процедуры анализа и оценки рисков.

ОСНОВНАЯ ЧАСТЬ

В документе НДТЗИ 1.1-003-99 риск определен как функция вероятности реализации определенной угрозы, вида и величины заданных убытков. Поскольку отдельные риски могут существенно отличаться в зависимости от типов рассматриваемых объектов, условий эксплуатации систем, этапов жизненного цикла, подходы к управлению рисками, могут различаться глубиной и уровнем формализации.

Под управлением рисками подразумевают скоординированные действия по руководству и управлению организацией в области риска. Процесс управления информационной безопасностью включает определение контекста, оценку рисков, обработку рисков, принятие рисков, коммуникацию рисков, а также мониторинг и пересмотр рисков. Процесс, объединяющий идентификацию, анализ и сравнительную оценку риска, называется оценкой риска. Оценка рисков усложняется также необходимостью учитывать ряд факторов: постоянное появление новых угроз информационной безопасности, ускорение темпов внедрения новых технологий автоматизации деятельности предприятия, возможную потерю актуальности данных, полученных в ходе анализа рисков. Оценивание рисков заключается в определении их количественных и качественных значений, формировании реестра рисков и ранжировании рисков.

Оценка рисков подразумевает ряд методов, с помощью которых можно дать объективную оценку, такие как:

- Экспертные;
- Теоретико-вероятностные;
- Вероятностно-статистический;
- Статистические.

Остановимся на подробном рассмотрении экспертных методов оценки. Под данной методикой в общем случае подразумевается заслушивание мнений экспертов и регистрацию в качественной или количественной форме суждений экспертов относительно какого-либо объекта, рассматриваемого в рамках данной проблемы. Технологию оценивания рисков экспертов можно рассмотреть в виде алгоритма (рис.1).

Экспертный метод применяется в случае, если необходимо выбрать решение, которое не может определяться только на основе точных расчетов. Достоинством такого метода является:

- Возможность охвата больших групп;
- Простота организации;
- Использование статистической обработки.

Особенность метода экспертных оценок в том, что данный метод базируется на заключениях экспертов в той или иной отрасли. Но, как и любой метод, метод экспертных оценок имеет свои недостатки:

- Возможность неправильного понимания вопросов;
- Неполнота ответов;
- Субъективные факторы опрашиваемых людей.

Проведение опроса является основным этапом работы экспертной группы, но перед его началом происходит анализ исследуемой задачи, обработка полученных данных и, основываясь на полученных сведениях, проводится экспертиза, которая рассматривается как последний шаг анализа. На этом шаге получают приближенное решение задачи или информацию по данной задаче, которая потом может либо использоваться в дальнейших вычислениях, либо являться окончательным решением.

На первом этапе проведения экспертных оценок выполняются следующие шаги:

- Решение административных и организационных вопросов;
- Формулировка проблемы и предоставление анкеты экспертам;

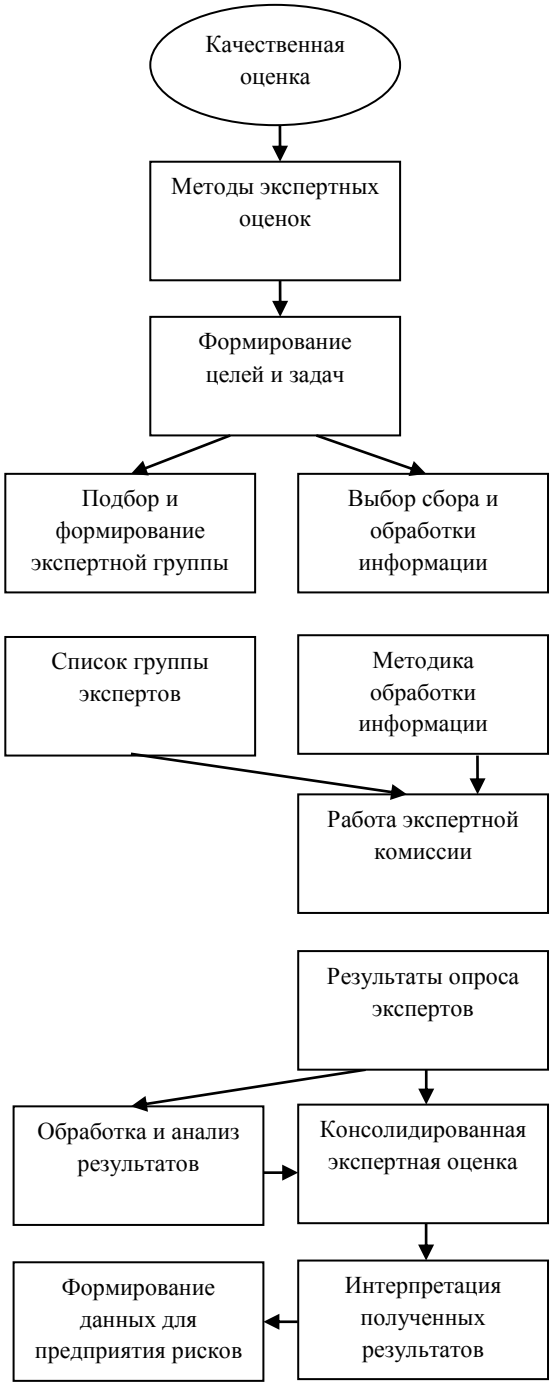

Рисунок 1. Алгоритм технологии экспертного оценивания рисков.

- Информационная поддержка работы экспертной группы.

При проведении опросов, основанных на суждениях о предпочтении объектов (решений, рисков) могут быть использованы следующие **виды экспертных оценок**:

1. Классификации;
2. Ранжирование;
3. Парные сравнения;
4. Баллы.

Обработка классификаций используется для построения иерархической структурной схемы факторов, влияющих на объект исследования. На первом уровне схемы размещают комплексные факторы, которые потом разделяются на более подробные и так далее до единичных факторов, которые затем и будут оценивать эксперты.

Ранжирование. Метод представляет собой процедуру упорядочения объектов, выполняемую экспертом. На основе знаний и опыта эксперт располагает объекты в порядке предпочтения, руководствуясь одним или несколькими выбранными показателями сравнения. В зависимости от вида отношений между объектами возможны различные варианты упорядочения объектов.

Метод парных сравнений заключается в том, что каждому эксперту предлагаются объекты парами, т.е. каждый объект сравнивается со всеми остальными, и эксперту необходимо выбрать из каждой пары объектов наиболее предпочтительный. В результате опроса получается матрица парных сравнений индивидуальная для каждого эксперта.

Бальные оценки используются, при определении зависимости между значениями единичных показателей объектов и значениями их оценок в баллах. Экспертам предоставляется бальная шкала, диапазон которой и градация зависит от решаемой задаче и необходимой точности ответа.

ВЫВОД

В настоящее время все шире применяются различные методы экспертных оценок. Они незаменимы при решении сложных задач оценивания и выбора технических объектов, в том числе специального назначения, при анализе и прогнозировании ситуаций с большим числом значимых факторов - всюду, когда необходимо привлечение знаний, интуиции и опыта многих высококвалифицированных специалистов-экспертов.

Рассмотрены виды экспертных оценок, каждый вид применяется к определенному методу оценки рисков.

Использование метода экспертных оценок помогает формализовать процедуру сбора, обобщения и анализа мнений специалистов с целью преобразования их в форму, наиболее удобную для принятия обоснованного решения.

СПИСОК ЛИТЕРАТУРЫ

1. НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу";
2. Н.И. Белоконь. Некоторые задачи экспертных оценок и их роль в корпоративном планировании. – режим доступа: http://jurnal.org/articles/2007/polit32.html;

УДК 004.056

СИСТЕМЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ОТ ВНУТРЕННИХ УГРОЗ

Малик Александр Игоревич[1], Баранов Анатолий Анатольевич
Государственный ВУЗ «Национальный горный университет», http://bit.nmu.org.ua/,
E-mail: nogoodforme@ya.ru[1]

Доклад посвящен актуальной на сегодняшний день теме предотвращения утечек конфиденциальной информации из информационной системы. Дается понятие о технологии *DLP*-систем, описание используемых в них методов анализа информации, их достоинств и недостатков.

Ключевые слова – конфиденциальная информация; лингвистический анализ; статистические методы; DLP-системы; лингвистический анализ; статистический анализ; информационная безопасность; хеш; канал утечки информации; политика информационной безопасности.

ВВЕДЕНИЕ

В настоящее время одной из наиболее актуальных угроз в области информационной безопасности является утечка конфиденциальных данных из-за несанкционированных действий пользователей.

Противодействовать утечке конфиденциальной информации компании помогают DLP-системы - программные или программно-аппаратные средства, предназначенные для защиты от утечек по сетевым и локальным каналам.

DLP-системы предназначены для отслеживания и блокирования попыток несанкционированной передачи данных за пределы корпоративной сети. Помимо предотвращения утечек информации DLP система может выполнять функции по отслеживанию действий пользователей, записи и анализу их коммуникаций через электронную почту, социальные сети, чаты и т.д.

ЗАДАЧИ

Основная задача систем DLP – обеспечение выполнения принятой в организации политики конфиденциальности.

Основные функции DLP-систем:

- контроль передачи информации через Интернет с использованием HTTP, HTTPS, FTP, и других протоколов;
- контроль сохранения информации на внешние носители - CD, DVD, flash, мобильные телефоны и т.п.;
- защита информации от утечки путем контроля вывода данных на печать;
- блокирование попыток отправки/сохранения конфиденциальных данных, информирование администраторов ИБ об инцидентах, создание теневых копий;
- поиск конфиденциальной информации на рабочих станциях и файловых серверах по ключевым словам, меткам документов, атрибутам файлов и цифровым отпечаткам;
- предотвращение утечек информации путем контроля жизненного цикла и движения конфиденциальных сведений.[1]

КАК РАБОТАЮТ DLP-СИСТЕМЫ

Технологии категоризации информации составляют ядро DLP-систем. В основном для категоризации данных в продуктах по защите корпоративной информации от утечек используются две основных группы технологий – лингвистический (морфологический, семантический) анализ и статистические методы (Digital Fingerprints, Document DNA, антиплагиат). Каждая технология имеет свои сильные и слабые стороны, которые определяют область их применения.

ЛИНГВИСТИЧЕСКИЙ АНАЛИЗ

Лингвистический анализ первым начал применяться при построении DLP-систем. Поиск осуществляется по ключевым словам и регулярным выражениям. Суть его заключается в том, что создаются списки ключевых слов и регулярных выражений, на основании которых осуществляется обнаружение конфиденциальной информации в потоке данных.

Большинство современных систем лингвистического анализа используют не только контекстный анализ, но и семантический анализ текста. Эти технологии работают тем эффективнее, чем больше анализируемый фрагмент. На большом фрагменте текста точнее проводится анализ, с большей вероятностью определяется категория и класс документа. При анализе же коротких сообщений (SMS, интернет-пейджеры) ничего лучшего, чем стоп-слова, до сих пор не придумано.

Достоинства лингвистических технологий:

- работают напрямую с содержанием документов, не важно, где и как был создан документ, какой на нем гриф и как называется файл;
- обучаемость;
- масштабируемость, скорость обработки информации пропорциональна ее количеству и абсолютно не зависит от количества категорий.

Недостатки лингвистических технологий:

- зависимость от языка;
- не вся конфиденциальная информация находится в виде связных текстов;
- вероятностный подход к категоризации;
- сложность разработки.

СТАТИСТИЧЕСКИЕ МЕТОДЫ АНАЛИЗА

Статистические технологии относятся к текстам не как к связной последовательности слов, а как к

произвольной последовательности символов, поэтому одинаково хорошо работают с текстами на любых языках. Поскольку любой цифровой объект – хоть картинка, хоть программа – тоже последовательность символов, то те же методы могут применяться для анализа не только текстовой информации, но и любых цифровых объектов. И если совпадают хеши в двух аудиофайлах – наверняка в одном из них содержится цитата из другого, поэтому статистические методы являются эффективными средствами защиты от утечки аудио и видео.

Ключевой характеристикой сложного хеша, снимаемого с защищаемого объекта (Digital Fingerprint, Document DNA), является шаг, с которым снимается хеш. Такой "отпечаток" является уникальной характеристикой объекта и при этом имеет свой размер. От шага хеша зависит размер такого отпечатка – чем меньше шаг, тем больше отпечаток. Если снимать хеш с шагом в один символ, то размер отпечатка превысит размер самого образца. Если для уменьшения "веса" отпечатка увеличить шаг (например, 10000 символов), то вместе с этим увеличивается вероятность того, что документ, содержащий цитату из образца длиной в 9900 символов, будет конфиденциальным, но при этом проскочит незаметно.

Достоинства статистических методов анализа:

- система не берет на себя ответственность за категоризацию документов;
- независимость от языка текста и нетекстовой информации.

Недостатки статистических методов анализа:

- перекладывается на пользователя ответственность за обучение системы, если конфиденциальный файл оказался не в том месте либо не был проиндексирован, то система его защищать не будет;
- физический размер отпечатка, при долгой эксплуатации системы растет количество отпечатков-образцов, что существенно замедляет работу;
- время снятия отпечатка напрямую зависит от размера файла, оно может превысить время неизменности объекта.[3]

СПОСОБЫ ПРИМЕНЕНИЯ

Первый способ называется граничным DLP (Border DLP). Запрещается вынос или отправка документов за границы организации. Когда пытаются вынести или отправить документ за границы организации каким-либо путем – по сети, через USB-диск (флешку), по почте и так далее, определяется его сигнатура и сравнивается с базой защищаемых документов. Если сигнатура в базе найдена, операция блокируется, а ИТ-безопасность уведомляется.

Второй способ называется агентским (Agent DLP). На каждый компьютер в организации устанавливается агент, отслеживающий всякую попытку работы с любыми документами (открытие, копирование, удаление, печать и т. д.). При каждой такой попытке он вычисляет сигнатуру документа, сравнивает ее с базой сигнатур. Если документ защищен, определяется пользователь, пытающийся с ним работать, и есть ли у этого пользователя права на выполнение этой операции. Если права есть, операция выполняется, если нет, блокируется и уведомляется служба безопасности.

Третий способ имеет общее название – DRM (Digital Rights Management), управление цифровыми правами. Данная технология реализуется путем встраивания механизма шифрования/дешифрации в стандартные программы для просмотра и редактирования документов. Клиентская часть при попытке открытия документа обращается с информацией о документе и открывающем его пользователе к серверу ключей, который хранит сведения о правах различных пользователей на доступ к различным документам. Если право на доступ есть, отправляется ключ, с помощью которого клиент незаметно для пользователя расшифровывает документ и дает возможность выполнить разрешенные операции.[4]

ЗАКЛЮЧЕНИЕ

Преимущества одной технологии проявляется там, где слаба другая. Лингвистика отлично работает с текстами, статистические методы – с другими форматами хранения информации.

Поэтому следует использовать в своих разработках обе технологии одновременно. В идеале использовать две эти технологии нужно не параллельно, а последовательно. Например, отпечатки лучше справятся с определением типа документа – договор это или балансовая ведомость, например. Затем можно подключать уже лингвистическую базу, созданную специально для этой категории. Это сильно экономит вычислительные ресурсы.

Решение DLP не должно быть сосредоточено только на одном канале утечек. Это должно быть комплексное решение, охватывающее максимальное количество каналов. При этом система должна обладать унифицированными средствами управления всех компонентов, которые она в себя включает.

Следует помнить, что DLP-системы эффективно работают только в комплексе с продуманной политикой информационной безопасности.[2]

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конеев И.Р., Беляев А.В., Информационная безопасность предприятия. 2003.
2. Вертузаев М.С., Юрченко О.М., Защита информации в компьютерных системах от несанкционированного доступа.
3. Независимый информационно-аналитический центр, полностью посвященный информационной безопасности (Электрон. ресурс) / Способ доступа: URL: http://www.anti-malware.ru/
4. Коллективный блог, раздел Информационная безопасность (Электрон. ресурс) / Способ доступа: URL: http://habrahabr.ru/hub/infosecurity/

УДК 004.056

АНАЛІЗ ВПЛИВОВИХ ФАКТОРІВ ДЛЯ СИСТЕМ АКТИВНОГО ЗАХИСТУ ВІД ВИТОКУ ОПТИКО-ЕЛЕКТРОННИМ КАНАЛОМ

Лебедько М.В., Кручінін О.В.
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/,
E-mail: lebedkomarina@gmail.com

У даній публікації розглядаються особливості використання активних засобів захисту від витоку оптико-електронним каналом. Наводиться аналіз позитивних і негативних факторів при роботі активних засобів захисту.

Ключові слова: оптико-електронний канал, вібровипромінювач, система активного захисту, мовна інформація.

ВСТУП

Проблема протидії зйому інформації з використанням лазерного випромінювання на сьогодні є досить актуальною і у той же час найменш дослідженою у порівнянні з іншими, менш «екзотичними» засобами промислової розвідки.

Для несанкціонованого отримання мовної інформації все частіше використовують дистанційні портативні засоби акустичної розвідки. Найбільш поширеними на сьогодні є лазерні системи акустичної розвідки, які дозволяють відтворювати мову, будь-які інші звуки та акустичні шуми при лазерно-локаційному зондуванні віконного скла та інших віддзеркалюючих (відбиваючих) поверхонь.

АНАЛІЗ ФІЗИЧНОЇ ПРИРОДИ ОПТИКО-ЕЛЕКТРОННОГО КАНАЛУ ТА ФАКТОРІВ, ЩО ВПЛИВАЮТЬ НА АКТИВНІ ЗАСОБИ ЗАХИСТУ

В оптико-електронному каналі джерелом витоку інформації є звичайне віконне скло (також скляна поверхня, дзеркало). Під дією мовного сигналу віконне скло (чи будь-яка інша тонка відбиваюча поверхня) здійснює низькочастотні коливання, якими може бути промодульоване високочастотне лазерне випромінювання. Відбите випромінювання потім сприймається фотоприймачем (детектором), котрий відновлює мовну інформацію з приміщення. Таким чином утворюється канал витоку мовної інформації. В даному випадку віконне скло є мембраною.

У техніці прийнято вважати, що мембрана – це гнучка або пружна, закріплена по замкненому контуру перетинка, що розділяє дві порожнини з різним тиском або відокремлює замкнену порожнину від навколишнього середовища. Постає питання, чи завжди віконне скло є мембраною, яка утворює оптико-електронний канал витоку інформації, та наскільки небезпечним (імовірним, зручним) є такий канал витоку. Для відповіді на ці питання треба дослідити вплив наступних параметрів :

1) співвідношення товщини скла (поверхні) до його площі;
2) спосіб закріплення скла;
3) форма скла (поверхні).

Також варто зазначити, що якість поверхні впливає на якість інформації, що знімається. Так зняття інформації з нового пластикового склопакета є простішим, аніж зі старих вікон, поверхня яких є нерівною. Такі поверхні сприяють дифузному відхиленню лазерного променя розвідувального пристрою, що робить зйом інформації малоймовірним.

Для протидії несанкціонованому отриманню мовної інформації за допомогою оптико-електронного каналу використовуються і активні, і пасивні методи. До пасивних методів відноситься використання штор, самоклейких металізованих плівок, жалюзі, відвертання шаф та інших предметів, що мають скляні поверхні. Через те що пасивні методи в більшості випадків впроваджуються на етапі будівництва, є затратними, а у ряді випадків для пасивних методів характерна демаскуюча ознака, активні засоби захисту від витоку мовної інформації є досить розповсюдженими.

До активних методів відноситься акустичне маскування. При використанні активних засобів слід враховувати, що засоби акустичного маскування можуть створюють негативний вплив на працівників, знижувати працездатність.

В Україні існують сертифіковані технічні засоби захисту мовної інформації [1], які можуть використовуватися для захисту інформації від витоку оптико-електронним каналом, але вони призначені для захисту інформації від витоку акустичним або віброакустичним каналом. Українські виробники технічних засобів пропонують готові комплекти для захисту інформації від витоку акустичним і віброакустичним каналами. Загалом до таких комплектів входять генератори, акусто- та вібровипромінювачі. Наприклад, один із рекомендованих копмлексів віброакустичного захисту складається з:

1) генератора шумових сигналів (акустичних і віброакустичних перешкод\завад) – МАРС ТЗО-4-2;
2) вібровипромінювача ВІ-3 (для установки на вікна);
3) вібровипромінювачаВІ-4 (для установки на стіни);
4) вібровипромінювача ВІ-4 (для установки на труби системи опалення);
5) акустичного випромінювача МАРС-АК;
6) акустичного випромінювача МАРС-АКЗ;
7) пристрою захисту телефонних ліній «Базальт-3»;
8) пульту дистанційного керування з виконуючим пристроєм.

У рекомендаціях щодо монтажу вібровипромінювачів виробники радять встановлювати один вібровипромінювач на одну поверхню або на раму, при цьому не враховується

площа поверхні. Радіус ефективної дії вібровипромінювачів становить 1,5 – 5 м при товщині скла 0,25 см. Для порівняння: російські виробники радять встановлювати один вібровипромінювач на одну скляну поверхню або раму, або декілька випромінювачів, якщо площа скла велика [2]. При цьому не вказується , яка площа скляної поверхні може вважатися великою. Також невідомо, яким чином впливають вібровипромінювачі один на інший, чи може робота одного нівелювати роботу іншого (інших), чи можливі «мертві» зони. Всі вищенаведені фактори впливають на ефективність захисту мовної інформації. Таким чином, в реальних умовах спеціаліст з технічного захисту інформації при встановленні вібровипромінювачів не має чітких обґрунтованих рекомендацій щодо їх монтажу.

При використанні засобів активного захисту виникає проблема оцінки вразливості приміщення щодо витоку інформації оптико-електронним каналом та оцінки ефективності впроваджених засобів захисту.

Таким чином, при впровадженні засобів активного захисту необхідно відповісти на наступні питання:

1) який ступень впливу засобів активного захисту один на інший за рахунок інтерференції;

2) який механізм контролю працездатності (виходу з ладу) вібровипромінювачів необхідно застосовувати (окрім контролю цілісності електричних ланцюгів);

3) який ефективний радіус дії вібровипромінювачів та яка кількість їх необхідна для конкретного об’єкта приміщення;

4) яка залежність між параметрами вікна (товщиною скла, його формою, якістю його поверхні, способу його закріплення) та параметрами вібровипромінювачів.

Для відповіді на поставлені питання, на першому етапі необхідно провести моделювання роботи систем активного захисту від витоку мовної інформації за рахунок оптико-електронного каналу

Розроблена система моделювання повинна забезпечувати можливість встановлення наступних параметрів:

- характеристики конструкції вікна (розмір, форма, способи кріплення скла, товщина та матеріал скла);
- характеристики вібровипромінювачів (потужність, спектр сигналу, направленість);
- взаємне розташування вібровипромінювачів.

При цьому повинна бути реалізована можливість контролю та індикації параметрів (спектральних та енергетичних характеристик) коливань скла на всій поверхні вікна, яке моделюється.

Для моделювання можна використовувати як потужні програмні пакети Mathcad чи Mathlab, що дозволяють візуалізувати та наглядно представити досить складну модель, так і програмні продукти, які створені з метою комп’ютерного моделювання механічних хвиль, якими є звук, – наприклад LongWave (моделювання продольних хвиль) та DiaWave (моделювання поперечних хвиль). Використання програмного пакета Матлаб є більш зручним, так як дозволяє створювати більш складні моделі, ніж LongWave та DiaWave [3], а також дозволяє проводити необхідні математичні операції над результатами, які дає модель в єдиному середовищі, та при необхідності візуалізувати їх без додаткових перетворень.

Результати моделювання будуть використані для розробки рекомендацій з проектування, монтажу та експлуатації систем активного захисту від витоку мовної інформації за рахунок оптико-електронного каналу.

ВИСНОВКИ

Активні засоби захисту від витоку мовної інформації оптико-електронним каналом є досить поширеними. Однак існують, недосліджені фактори, що чинять вплив на роботу цих засобів. За допомогою моделювання можна провести дослідження впливових чинників та розробити рекомендації з проектування, монтажу та експлуатації систем активного захисту від витоку мовної інформації за рахунок оптико-електронного каналу.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Перелік засобів забезпечення технічного захисту інформації загального призначення, на які Держспецзв'язку погоджено технічні умови (Електрон. ресурс) / Спосіб доступу: URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=77941&cat_id=39181/ - Загол. з екрана

2. Система виброакустической и акустической защиты «Соната-АВ» (Електрон. ресурс) / Спосіб доступу: URL: http://www.cbi-info.ru/files/sonata-av3m.pdf - Загол. з екрана

3. Компьютерное моделирование механических волн (Електрон. ресурс) / Спосіб доступу: URL: https://sites.google.com/site/wavecommod/ - Загол. з екрана

УДК 004.056

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ПРОЦЕСУ ОБРОБКИ РИЗИКІВ

Начовна Д.А., Мартиненко А.А.

Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/,

E-mail:darja.tkacevich@gmail.com

Робота присвячена аналізу методів обробки ризиків, як одного з ключових етапів процесу управління ризиками інформаційної безпеки. Обробка ризиків – складний інформаційномісткий процес, який можливо спростити та зробити структурованим за допомогою систем підтримки прийняття рішення, зокрема стратегічних.

Ключові слова – обробка ризиків, методи

обробки ризиків, система підтримки прийняття рішень, інформаційна безпека, управління ризиками інформаційної безпеки.

ВСТУП

Управління ризиками – високе мистецтво. Світова практика показує, що єдина можливість запобігання будь-якої світової кризи та збереження стабільності – оволодіти мистецтвом управління ризиків. Сфера інформаційної безпеки не є виключенням.

Важливими нагальними питаннями в управлінні ризиками інформаційної безпеки залишаються основні його етапи: оцінка ризиків та обробка ризиків. Що цікаво, сьогодні не існує єдиного шаблонного варіанту щодо визначення основних стовпів управління ризиками. Більше того, державні законотворці та регулятори мають тенденцію ускладнювати і без того тернистий пошук ідеального балансу досягнення інформаційної безпеки та пов'язаними з цим перевагами, при цьому зберігаючи правильне інвестування та залишаючись конкурентноспроможними, ефективними, успішними та рентабельними. Подібний баланс кожна організація вимушена шукати індивідуально.

ОБРОБКА РИЗИКІВ

Тож, процес обробки ризиків є одним з головних етапів управління ризиків інформаційної безпеки, метою якого є або максимальне зниження вірогідності реалізації такого, або мінімальна величина збитку, який може понести компанія. На перший погляд може здатись, що достатньо легко можна досягти досить прозорої кінцевої мети. Проте практика показує, що максимальний ефект в обробці ризиків досягається синтезом, і в кожному конкретному випадку, навіть маючи схожі вихідні данні, синтез рішень зовсім не обов'язково буде шаблонним.

Залежно від того, чи відбуватимуться зміни характеристик ризиків, можна виділити регулювання та фінансування ризиків.

До регулювання ризиків відносяться методи, в результати яких відбувається цільова зміна таких характеристик ризику, як ймовірність, наслідки або розкид можливих результатів. Фінансування ризику має на меті компенсацію наслідків реалізації ризику, без зміни його властивостей.

Залежно від того, що буде відбуватись з ризиком після впровадження наступних методів, оцінку ризиків можна розділити на 4 категорії [1] (див. Табл.1):

- прийняття ризику;
- зменшення ризику;
- перекладання ризику;
- уникнення ризику.

Таблиця 1. Класифікація методів обробки ризику

Метод	**Що відбувається з ризиком**
Прийняття ризику	Ризик продовжує існувати та повністю залишається у даного суб'єкта
Зменшення ризику	Ризик продовжує існувати у даного суб'єкта, проте змінюється (зменшується) його рівень (зазвичай кількісна характеристика)
Перекладання ризику	Ризик продовжує існувати, проте всі або окремі його компоненти передаються іншим особам
Уникнення ризику	Ризик перестає існувати у даного суб'єкта

1. Рішення про прийняття ризику для починаючого високотехнологічного підприємства набагато ймовірніше, аніж для солідної організації стандартної орієнтації. Кожна організація має встановити власні критерії прийняття ризиків, тим самим визначити максимально припустимий залишковий ризик. Всі ризики, що перевищують припустимий залишковий, мають автоматично не прийматись. Іншій ж мають пройти через детальний кількісний та якісний аналіз ризиків.

2. Рішення про зменшення ризиків розглядають завжди першочергово, коли ризик є неприйнятним. Мова йде про зменшення ризику до максимально прийнятного значення шляхом використання механізмів контролю. Останні можна знайти в міжнародних стандартах ISO 27001 та ISO 27002, котрі містять опис та керівництво по застосуванню для кожного з механізмів контролю. Крім стандартів серії ISO 2700x та інших серій, в нагоді можуть бути й інші міжнародні стандарти. Наприклад, німецькі стандарти серії BSI/IT - Baseline Protection Manual.

Вибір механізма контролю, як і будь-який інший вибір, треба обґрунтовувати. Якісним показником економічної доцільності використання того чи іншого методу, його ефективності та реалізує мості може слугувати коефіцієнт повернення інвестицій (ROI), що обчислюється за формулою (1):

$$ROI = (Зменш.\ середньорічних\ втрат - Вартість\ захисних\ заходів) / Вартість\ захисних\ заходів, \quad (1)$$

Якщо коефіцієнт повернення інвестицій від'ємний (ROI<0), це свідчить про те, що засоби захисту інформації дорожчі безпосередньо за інформацію. В такому разі треба переглянути комплекс захисту.

3. Якщо зменшення ризику до певного рівня є проблематичним, можна використати метод передачі ризику третій стороні. В цьому випадку третьою стороною можуть виступити страхові фірми чи аутсорсингові компанії. При передачі ризику особливу увагу треба звертати на юридичну сторону оформлення, адже від цього залежить своєчасність і повнота виплати в разі настання страхового випадку. Не треба забувати і про залишкові ризики, які не можливо виключити в даному методі. Це пов'язано з тим, що страхування в сфері інформаційної безпеки тільки починає розвиватись в Україні і ще немає чіткого визначення страхового випадку за подією інформаційної безпеки. На сьогоднішній день неможливо застрахувати ризики, пов'язані з технологічними помилками, ризики при реалізації проектів та кібер-ризики.

Для того, щоб в Україні страхування ризиків ІБ мало успішну практику, необхідно подолати наступні етапи становлення:

- створити методологію оцінки рівня збитків від витоку інформації з обмеженим доступом;
- створити власну актуальну і не суперечливу законодавчу базу, котра б детально описувала процес страхування інформаційних ризиків;

- вимоги національних українських документів з інформаційної безпеки повинні бути орієнтовані не тільки на державні структури, а й на бізнес;
- не допускати введення цензури в країні, щоб у міжнародної спільноти створювалося об'єктивне уявлення про ситуацію в Україні, тим самим забезпечити входження України у світовий інформаційний простір.

4. Уникнення ризику є доцільним, коли є можливість відносно безболісної реорганізації бізнесу. Це можуть бути рішення про відмову обробляти певну конфіденційну інформацію, про відмову від деяких запланованих бізнес-активностей або перенесення власних ресурсів з зони ризику. Проте варто пам'ятати принцип ведення бізнесу, коли професійніше – навчитися управляти ризиками, а не шукати можливості уникнути таких.

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ ДЛЯ ПРОЦЕСУ ОБРОБКИ РИЗИКІВ – ПРИНЦИП ТАКСОНОМІЇ

Так, як способи обробки ризиків не є взаємовиключними, а вибір способу синтезу методів обробки ризиків є складним завданням, при цьому границі між основними чотирма методами обробки ризику є досить умовними та тонкими, то є потреба застосовувати систему підтримки прийняття рішення.

Система підтримки прийняття рішення [2] - це інтерактивні автоматизовані інформаційні системи, які допомагають особам, що приймають рішення, використовувати дані та моделі для того, щоб вирішувати неструктуровані та слабко структуровані проблеми (задачі).

В СППР використовують останні рішення в галузі інформаційних технологій: сховища та вітрини даних, OLAP-технології, нейромережі, штучний інтелект, генетичні алгоритми, добування знань (Data Mining).

Існує безліч класифікацій СППР. Та в випадку з аналізом значних обсягів різнорідної інформації, що збираються з різних джерел, краще використовувати стратегічні СППР. Найважливішою метою стратегічних систем підтримки прийняття рішення є пошук найбільш раціональних варіантів розвитку із урахуванням багатофакторного. Головною перевага такої системи - можливість менеджерам компанії обґрунтовувати свої рішення на основі аналізу великих масивів інформації.

Якщо провести аналогію поміж СППР та таксономією [3], то системи підтримки прийняття рішення є простішими в реалізації, при цьому принципи залишаються спільними – класифікація та систематизація складно організованих областей дійсності.

ВИСНОВКИ

Прийняття остаточного рішення в питанні обробки ризиків хибно вважають обов'язком спеціаліста з захисту інформації. Адже відповідальність за вибір тієї чи іншої моделі обробки ризиків можна порівняти з типовим бізнес-рішенням, котре має приймати керівник організації. Зазвичай, подібні рішення є ключовими і ведуть за собою зміни в роботі, а інколи і звичному функціонуванні установи.

Зрозуміло, що попередньо керівник має володіти повною, достовірною, підкріпленою фактами інформацією про наступне:

- наявність та рівень серйозності проблеми;
- наслідки у випадку відсутності будь-якої реакції на виклики;
- запропоновані рішення (обов'язково має бути декілька, так як альтернатива є завжди і керівник має право та обов'язок самостійно обирати);
- наявність і рівень залишкового ризику.

Наступним кроком після прийняття рішення має стати розробка плану обробки ризиків. Створення такого документу, реалізація та контроль за виконанням покладається на спеціаліста з інформаційної безпеки. Найчастіше таким документом слугує «Декларація про застосування механізмів контролю».

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Астахов Александр, Искусство управления информационными рисками. М.: ДМК Пресс, 2010. – 312 с.

2. Бідюк П.І., Гожий О.П., Коршевнюк Л.О., Комп'ютерні системи підтримки прийняття рішень. (Електрон. ресурс) / Спосіб доступу – http://lib.chdu.edu.ua/pdf/posibnuku/313/3.pdf - Заголовок з екрана.

3. Черешкин Д.С., Принципы таксономии угроз безопасности информационных систем. (Електрон. ресурс) / Спосіб доступу – http://www.iso27000.ru - Заголовок з екрана.

УДК 004.056

АНАЛІЗ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОПЕРАЦІЙ БЕЗКОНТАКТНИХ ПЛАТЕЖІВ MASTERCARD PAYPASS

Францевич-Скарбовська Д.Ю.[1], Кручінін О.В[2]

Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, vendetta@gmail.com[1], rubin13@i.ua[2]

У поданій статті піднята проблема співвідношення швидкості та безпечності безготівкого безконтактного розрахунку за допомогою технології PayPass. Також описано увесь процес обробки платежу, наведено загрози безпеки властивостям інформації та зроблено пропозиції щодо покращення рівня захищеності.

Ключові слова : технологія PayPass MasterCard, безконтактний звязок, інформаційна безпека.

Виникнення безготівкового розрахунку припадає на 40-50-ті роки минулого століття у часи «торгівельного буму» у США, коли клерки банку фізично не могли впоратися з великою кількістю паперу, якою супроводжувалися запити на кредит та

їх узгодження, тому було вирішено створити систему самообслуговування клієнтів за допомогою карток, а вже пізніше карток і банкоматів. В наш час за способом ідентифікації розрізняють декілька видів банківських карток: картки з магнітною стрічкою, з інтегрованим чіпом, безконтактні, а також комбіновані. Великої популярності нині набирають картки, оздоблені можливістю розраховуватися безконтактно, тільки один банк в Україні випустив до 2012 року більш ніж 450 тис. карток. Такі масштаби поширення пояснюються в першу чергу швидкістю проведення операції: клієнт витрачає десь близько чотирьох секунд на оплату придбаного товару або отриманої послуги. Міжнародна платіжна система MasterCard у 2005 році запропонувала свій варіант безконтактного способу оплати технологією PayPass.

MasterCard PayPass - це сумісна з EMV (міжнародний стандарт для операцій з банківськими картами з чіпом) безконтактна можливість проведення платежу, заснована на стандарті ISO / IEC 14443, що надає власникам карток MasterCard PayPass і Maestro PayPass спосіб здійснення оплати шляхом близького піднесення або дотику платіжною карткою або іншим платіжним інструментом, таким як телефон або брелок для ключів, до зчитувального платіжному терміналу замість проведення нею для зчитування або вставки її в термінал [1].

PayPass карти і пристрої на базовому рівні складаються з антени підключеної до мікросхеми (чипу) у модулі. Ці компоненти зазвичай інкапсулюються (монтуються) в «носії» різних форм і розмірів.

Для карти MasterCard PayPas, компоненти містяться в листі пластика розміром з картку, відомого як inlay. Цей фрагмент пластику знаходиться між передньою і заднім листами пластика, формуючи готову карту.

Чіп PayPass кодується даними і містить криптографічні дані, які використовуються для аутентифікації карти або пристрою до емітенту (банк що випустив картку). пристрій, що зчитує робить енергію доступною чіпу шляхом індукування створюючи в повітрі навколо себе електромагнітне поле. Коли чіп поміщається в це поле, електрична енергія подається на нього за допомогою антени (спіраль з дроту). Ця енергія використовується для живлення чіпа; карти і пристрої PayPass не потребують батарей.

Інформація, надана чіпом PayPass приймається зчитувальним пристроєм PayPass, і відформатована відповідним чином, обробляється за допомогою існуючих POS систем продавця для авторизації, клірингу (безготівковий розрахунок між двома сторонами) і розрахунків за схемою зображеною на рисунку 1.

Обробка транзакції PayPass виконується наступним чином:

1. Термінал з підтримкою MasterCard PayPass зчитує PayPass CVC2, статичний CVC3 і 2 ключа для генерування динамічного CVC3 з картки або пристрою генерує динамічний CVC3 і відправляє всі перераховані вище дані для авторизації. Дані включають вказівку, що транзакція була набрана на сенсорному екрані, обрана з готового списку або набрана з клавіатури.

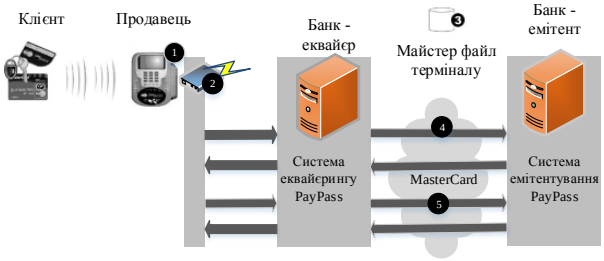

Рисунок 1. Процес обробки транзакції PayPass

2. Високошвидкісний система авторизації передає запит на авторизацію до банку-екваеру.

3. Якщо не передбачена авторизація за екваером, він може визначити, що термінал підтримує PayPass шляхом опитування майстром файлу терміналу.

4. Використовуючи коди авторизації MasterCard екваер розуміє, що дані були передані через термінал з підтримкою PayPass та передані були безконтакнтим методом.

5. Транзакція направляється в банк-емітент через авторизаційної мережу MasterCard.

6. Пункти 3,4 повторюються, коли транзакція записується в "системи MasterCard". Записуються POS режим введення (DE 22) і можливості терміналу (DE 61).

7. Вимоги до кодування операції PaPass визначені в MasterCard Global Operations Bulletin No. 6, 1 червня 2005.

З погляду безпеки прийняті наступні міри:

- Чіп PayPass не містить імені держателя картки.
- Записані на чіп PayPass відрізняються від значень на магнітній смузі. Термінал сам визначає потрібні дані для кожного варіанту платежу.
- Різні значення CVC при укладанні угоди за допомогою PayPass і операції з магнітною смугою.
- Використовуємий статичний код аутентифікації CVC3 відрізняється статичного CVC1 нанесеного на магнітну смугу.
- Прив'язаний до чіпу PayPass номер рахунку відрізняється від рахунку для магнітної смуги і контактного чіпа.

CVC2 та/або SecureCode - верифікація власника картки, запобігає використання номера рахунку і дати закінчення терміну дії картки при видачі дозволу на електронні операції.

Динамічний CVC3 – це генерований дискретний код аутентифікації для кожної транзакції. При розрахунку CVC3 використовується потрійний DES алгоритм з 112 - бітними ключами. Термінал зчитує ключі (які зберігаються у захищеній частині пам’яті чіпу) та генерує динамічний CVC3 код унікальний для кожної транзакції [3].

На основі аналізу схеми обробка транзакцій PayPass було виявлено основні загрози. У таблиці 1 наведено загрози властивостям інформації, що циркулює в системах з технологією PayPass MasterCard:

Таблиця 1. Загрози при використанні PayPass

Вразливість	**Загроза**	**Порушена властивість інфорації**

NFC+RFID (незахищений радіоканал)	Relay attack (різновид атаки "людина посередині" зловмисник відправляє жертві запит зчитувача і її відповідь в режимі реального часу і передає далі на зчитуваючий пристрій).	К, Д
NFC+RFID (використання радіоканалу для передачі даних)	Руйнування даних відносно легко здійснити засобами радіоелектронної боротьби (РЕБ).	Д
NFC+RFID (передача даних у незахищеному вигляді)	Прослуховування: радіочастотний сигнал бездротової передачі даних може бути перехоплений антенами.	К
NFC+RFID (незахищеність радіоканалу від підміни одного з учасників)	Атака з використанням експлойта 0day: можливо передати через NFC-з'єднання шкідливий файл і отримати повний контроль над пристроєм одержувача.	К, Д, Ц.
Потрійний DES+NFC+ RFID (радіоканал зв'язку та загальновідомість алгоритму шифрування)	Можлива атака з відомим відкритим текстом: передбачається, що противник знає криптосистему, тобто, алгоритми шифрування і дешифрування і противник отримує в своє розпорядження ще деякий набір кріптограм і відповідних їм відкритих текстів.	К
Потрійний DES+NFC+ RFID (радіоканал зв'язку та використання мережі Інтернет)	Проста атака з вибором відкритого тексту (chosen-plaintext attack). Передбачається, що противник має можливість вибрати необхідну кількість відкритих текстів і отримати їх криптограми. При цьому всі відкриті тексти повинні бути обрані заздалегідь, тобто, до отримання першого криптограми.	К

На даний момент існують способи щодо запобігання клонуванню карти (Physically Unclonable Functions) та для шифрування інформації що передається за допомогою радіоканалу (computational RFID) [2].

Використання безконтактної технології PayPass MasterCard значно економить час банків та їх клієнтів, якщо порівнювати її з оплатою готівкою або банківською картою інших видів, однак використовувані методи потенційно відкривають можливості для витоку персональної інформації, дублювання проведених платежів і небажаного копіювання банківської карти.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вікіпедія (Електрон. ресурс) / Спосіб доступу: URL: http://ru.wikipedia.org/wiki/MasterCard_PayPass. – MasterCard PayPass.

2. SecurityLab (Електрон. ресурс) / Спосіб доступу: URL: http://www.securitylab.ru/news/359135.php. – Американські вчені захистили RFID від клонування.

3. PayPass Mag Stripe Asquirer Implementation Requipments, 2012. – 1-7 с.

УДК 004.7:004.056

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ВИКОРИСТАННЯ КОНЦЕПЦІЇ BYOD В ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Стасівський Л.С., Масальська О.О.

ДВНЗ «Національний гірничий університет» http://bit.nmu.org.ua/, stasivskyj@gmail.com

У сучасній організації робочі місця багатьох співробітників перестають бути статичними. На сьогоднішній день є можливість підключатися до різних хмарних сервісів і використовувати можливості свого пристрою для виконання робочих операцій, буквально тримаючи в руках телефон, адже тепер комп'ютер, який стоїть на столі робітника, вже не має цінності. Маючи можливість виконувати ті ж робочі завдання, але за допомогою свого особистого пристрою, співробітник, як показує практика, буде прагнути це робити. Завдання ІТ-служби в компанії - забезпечити йому таку можливість.

Ключові слова – технологія Bring Your Own Device; безпека корпоративних даних.

ВСТУП

Концепція BYOD (Bring Your Own Device – Принеси Свій Власний Пристрій) – це підхід до організації робочого місця співробітника, при якому він застосовує власний пристрій для доступу до інформаційних ресурсів компанії.

Наскільки підхід виправдовує свої очікування, можна судити з того, як він активно застосовується в різних компаніях у всьому світі. Наприклад, згідно з дослідженням компанії Fortinet, 74% респондентів регулярно використовують особисті електронні прилади у виробничих цілях. Більш того, 55% з опитаних вважають таке використання особистих приладів своїм правом, а не привілеєм. А, за даними дослідження компанії Microsoft, найбільш лояльними до концепції BYOD є китайські компанії (86%) і найменш лояльними – японські (30 %). На рис. 1 представлено розподіл рівня лояльності компаній в різних країнах до концепції BYOD [1].

Синій (верх): концепція BYOD дозволена і вітається.

Блакитний: концепція BYOD дозволена, але не вітається.

Помаранчевий: концепція BYOD заборонена.

Коричневий (низ): концепція BYOD не регулюється.[1]

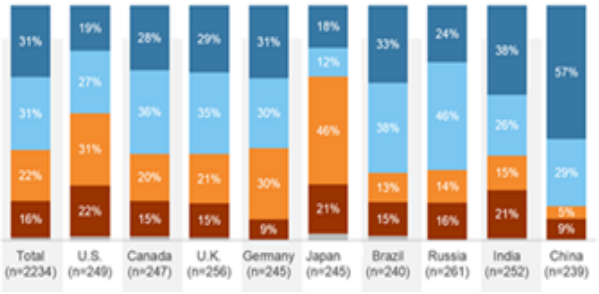

Рисунок 1. Розподіл рівня лояльності компаній в різних країнах до концепції BYOD

При прийнятті рішення про перехід компанії на використанні концепції BYOD необхідно проаналізувати наслідки впровадження данної технології. Особливу увагу потрібно звернути на забезпечення заходів безпеки, оцінити вплив BYOD на всю систему мережевої безпеки компанії, мати уявлення про проблеми які можуть виникнути.

Ноутбуки, планшети, смартфони які підключаються до корпоративні мережі, отримують доступ до веб-додатків і поштових систем, доставляючи чимало проблем IT адміністраторам і фахівцям з інформаційної безпеки.

Найбільш популярними рішеннями проблем інформаційної безпеки є використання інфраструктурі віртуальних робочих місць VDI (Virtual Desktop Infrastructure - Віртуальні Робочі місця), використання технології MDM (керування мобільними приладами).[2]

ВИКОРИСТАННЯ ВІРТУАЛЬНИХ РОБОЧИХ МІСЦЬ

Для вирішення поставлених завдань необхідно застосування гнучких збалансованих методів, замість заходів по повній забороні мобільних пристроїв в корпоративному середовищі.

Використання інфраструктури віртуальних робочих місць VDI (Virtual Desktop Infrastructure – віртуальні робочі місця) – віртуальні робочі місця, засновані на серверних рішеннях, представляють із себе користувальницькі додатки або цілі операційні системи, що працюють у віртуальному середовищі, під управлінням адміністратора, функціонуючого на централізованому сервері. Один фізичний сервер, на якому розгорнуте віртуальне середовище, може одночасно працювати з безліччю віртуальних робочих місць користувача, розгорнутих на його віртуальних машинах. Число одночасно підтримуваних віртуальних машин залежить від кількості пам'яті і обчислювальних ресурсів фізичного сервера. Такий підхід дуже зручний, оскільки забезпечує централізоване адміністрування і зберігання даних, дозволяє поступово нарощувати інфраструктуру, і, в міру необхідності, створювати, або видаляти робочі місця, а також легко переносити їх з одного сервера на інший. Перевагою застосування таких віртуальних робочих місць є високий захист корпоративних даних у віртуальному середовищі, надаючи, при цьому, користувачу високу свободу дій, відкриваючи доступ до корпоративних IT-ресурсів через захищене з'єднання, що запобігає витоку конфіденційних даних на пристроях користувачів.[3]

ВИКОРИСТАННЯ ДОДАТКІВ УПРАВЛІННЯ МОБІЛЬНИХ ПРИСТРОЇВ

Додатковим рішенням даної проблеми інформаційної безпеки є використання спеціального інструментарію для управління мобільними пристроями (MDM). Дана технологія за рахунок розмежування доступу MDM повинна була допомогти знайти баланс між перевагами працівників і потребою компаній захистити корпоративні дані організації, які впровадили MDM. Компанії що ввели цю технологію доходять висновку, що це ПЗ негативно позначається на досвіді користувача. По-перше, установка на особистий апарат деякий фрагмент коду, за допомогою якого можливо відправляти будь-які команди і настройки, викликає неприйняття персоналу. По-друге, смартфони та планшети спочатку розроблялися під споживчий сегмент, тобто з урахуванням максимальної зручності використання, і їх власники просто не готові миритися з появою яких недоліків.

MDM - далеко не єдиний інструмент, який дає можливість організувати роботу з персональними пристроями в корпоративному середовищі. Багатьом компаніям під силу обійтися і без нього, за рахунок онлайнових сервісів (у тому числі дистанційного видалення даних).[4]

ЗАГРОЗА ВТРАТИ МОБІЛЬНИХ ДАНИХ

Найбільша загроза для мобільних даних - крадіжка або втрата самого апарату, але для її вирішення існує безліч недорогих і навіть безкоштовних інструментів (Find My iPhone, Where's my Droid, пр.). Наприклад, компанії можуть використовувати безкоштовну утиліту Apple iOS Configuration Utility і каталог AppleID для автоматичної настройки Find My iPhone на користувацьких апаратах, а щоб не дати злодію відключити пристрій - застосовувати Device Restrictions. Звичайно, з обережністю, адже помилкові спрацьовування не виключені.

ВИСНОВОК

При впровадженні даної технології потрібно дотримуватися перерахованих вище методів вирішення проблеми інформаційної безпеки, а також для покращення захищеності корпоративних даних можливо застосовувати:

- Двуфакторную аутентифікацію.
- Безпечний віддалений доступ з допомогою SSL VPN.
- Підтримка обізнаності персоналу.

BYOD – це лише концепція, перехідна форма між класичним нерухомим комп'ютером на робочому столі і новим підходом до організації роботи з метою забезпечити максимальний комфорт і продуктивність працівника, давши йому можливість працювати там, тоді й таким чином, як йому буде зручно.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. BYOD – четыре буквы способные напугать даже крупную компанию (Електрон. ресурс) / Спосіб доступу: URL: http://vido.com.ua/article/3112/byod-chietyrie-bukvy-sposobnyie-napughat-dazhie-krupnuiu-kompaniiu/ - BYOD – четыре буквы способные напугать даже крупную компанию.

2. Что такое BYOD и насколько она эффективна в организациях? (Електрон. ресурс) / Спосіб доступу: URL: http://ecm-journal.ru/post/Chto-takoe-BYOD-i-naskolko-ona-ehffektivna-v-organizacijakh.aspx - Что такое BYOD и насколько она эффективна в организациях?

3. Bring Your Own Device с точки зрения интересов отечественного бизнеса (Електрон. ресурс) / Спосіб доступу: URL: http://www.cisco.com/web/RU/news/releases/txt /2012/112912c.html - Bring Your Own Device с точки зрения интересов отечественного бизнеса

4. Инфраструктура виртуальных ПК (Електрон. ресурс) / Спосіб доступу: URL: http://www.parallels.com/ru/solutions/vdi/ - BYOD – Инфраструктура виртуальных ПК

5. Управление основными данными (Електрон. ресурс) / Спосіб доступу: URL: http://ru.wikipedia.org/wiki – Управление основными данными.

УДК 004.056.53

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ПРЕОДОЛЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ С ПОМОЩЬЮ СЕТЕЙ ПЕТРИ

Нортенко Дмитрий Вячеславович
Государственное ВУЗ «Национальный горный университет», http://bit.nmu.org.ua/,
dimanortenko@gmail.com

В данной статье предложен общий подход моделирования, в котором сети Петри рассматриваются как вспомогательный инструмент анализа информационной системы.

Ключевые слова – моделирование систем защиты информации, сети Петри.

ВСТУПЛЕНИЕ

Теория сетей Петри применяется в различных областях, например, в параллельном и системном программировании, технологиях тестирования, экономике, менеджменте, сетевом планировании и т.д. Существует два основных практических применений сетей Петри в области информационной безопасности: использование при проектировании системы защиты информации и использование как инструмента моделирования для дальнейшего анализа системы.

Сети Петри – это математический аппарат для моделирования динамических дискретных систем. Сети Петри разрабатывались для моделирования систем с параллельными взаимодействующими компонентами.

Сеть Петри представляет собой двудольный ориентированный граф, состоящий из вершин двух типов – позиций и переходов, соединённых между собой дугами. Вершины одного типа не могут быть соединены непосредственно. Позиции могут содержать в себе метки, которые в свою очередь могут перемещаться по сети. Метки часто называют маркерами или фишками.

Под событием понимают срабатывание перехода, при котором метки из входных позиций этого перехода перемещаются в выходные позиции. События происходят мгновенно, либо разновременно, при выполнении некоторых условий. На рисунке 1 приведен наглядный пример сети Петри.

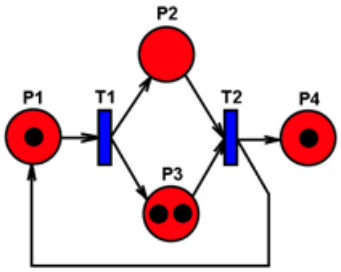

Рисунок 1. Простейший пример сети Петри

Большими кругами обозначены позиции, маленькими чёрными кругами – метки (фишки), прямоугольниками – переходы.

Процесс функционирования сети Петри может быть наглядно представлен графом достижимых маркировок. Состояние сети однозначно определяется её маркировкой – распределением фишек по позициям. Вершинами графа являются допустимые маркировки сети Петри, дуги помечены символом срабатывающего перехода. Дуга строится для каждого возбуждённого перехода. Построение прекращается, когда мы получаем маркировки, в которых не возбуждён ни один переход либо маркировки, содержащиеся в графе. Граф достижимых маркировок представляет собой автомат.

СЕТИ ПЕТРИ КАК ИНСТРУМЕНТ МОДЕЛИРОВАНИЯ

В настоящее время сети Петри применяются, в основном, в моделировании. Во многих областях исследований явление изучается не непосредственно, а косвенно, через модель. Модель – это представление, как правило, в математических терминах того, что считается наиболее характерным в изучаемом объекте или системе.

Развитие теории сетей Петри проводилось по двум направлениям. Формальная теория сетей Петри занимается разработкой основных средств, методов и

понятий, необходимых для применения сетей Петри. Прикладная теория сетей Петри связана главным образом с применением сетей Петри к моделированию систем, их анализу и получающимся в результате этого глубоким проникновением в моделируемые системы. [2]

Моделирование в сетях Петри осуществляется на событийном уровне. Определяются, какие действия происходят в системе, какие состояние предшествовали этим действиям и какие состояния примет система после выполнения действия. Выполнения событийной модели в сетях Петри описывает поведение системы. Анализ результатов выполнения может сказать о том, в каких состояниях пребывала или не пребывала система, какие состояния в принципе не достижимы.

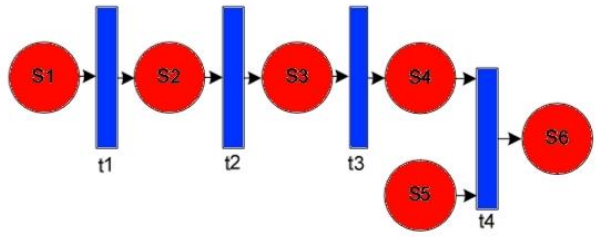

Рисунок 2. Пример сети Петри для угрозы перехвата чужих паролей легальным пользователем ОС

Основными проблемами, препятствующими прямой реализации модели являются неполнота информации о состоянии системы, сложность расчета переходных функций автомата, сложность аналитического представления функций выходов автомата.[3]

ПОСТРОЕНИЕ МОДЕЛИ ПРОЦЕССА РЕАЛИЗАЦИИ УГРОЗЫ

Предлагается модель, которая даст возможность оценить вероятность реализации угрозы, а также времени, необходимого для реализации определенной угрозы в информационной системе.

Рассматривается временная сеть Петри:

$N = (P_l, T, F, W, M_0)$, где P_l – множество мест сети $P_1 = S \cup \{V_1\} \cup T_h \cup F_1$, где S – злоумышленник, $\{V_l\}$ – уязвимости СЗИ, T_h – реализация угрозы. F_1 – провал попытки реализации угрозы. Множество переходов T представляет собой фактически множество способов эксплуатации той или иной уязвимости СЗИ.

Для времен переходов используется логнормальный закон распределения плотности вероятностей. Начальная разметка сети M_0 такова:

$M_0(P_{li}) = 0$ при $P_{li} \in S$, $M_0(S) = 1$.

Для разрешения конфликтов используется предварительный выбор по вероятности срабатывания перехода, которая интерпретируется как вероятность выбора злоумышленником данного способа эксплуатации уязвимости.

Анализ данной сети осуществляется моделированием. Моделирование проводится до достижения либо места T_h, либо F_l, либо до достижения сетью состьяния , в котором не сможет сработать ни один переход[4].

ВЫВОД

Сети Петри можно весьма успешно использовать для анализа и подробного исследования СЗИ. Модель, построенная с использованием теории сетей Петри отображает процессы преодоления СЗИ и ИС, используя коненчное число возможных состояний автомата. Управляя условиями в узлах сети Петри, получаем возможность моделировать разнообразные процессы преодоления защиты, которые злоумышленник, даже с самой малой вероятностью, может реализовать. Аппарат сетей Петри позволяет формализовать процесс исследования эффективности СЗИ.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. “Сети Петри” (Электрон. ресурс) / Режим доступа: http://wikipedia.org/wiki – Сети Петри;
2. Сравнительный анализ моделей систем защиты информации (Электрон. ресурс) / Режим доступа: http://inf-bez.ru/?p=767;
3 Математический аппарта сетей Петри-Маркова (Электрон. Ресурс) / Режим доступа: http://klax.tula.ru/~spm;
4. “Математическое моделирование распределенных систем защиты информации”, Давыдова Е.Н. (Электрон. ресурс) / Режим доступа: http://swsys.ru/index.php?page=article&id=2764;

УДК 004. 056.53

СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ: СТРУКТУРА ТА НАПРЯМИ ЇЇ ВДОСКОНАЛЕННЯ

Галушка Олексій Андрійович
Науковий керівник: асистент Баранов А.А.
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, E-mail: galushka@mail.ru

Розглядається структура сучасних систем виявлення вторгнень (СВВ). Характеризуються основні напрями розпізнавання порушень безпеки у системах, які захищаються в сучасних СВВ. Проведено аналіз використовуваних методів та моделей структури СВВ у відповідності з виділеними основними групами.

Ключові слова – система виявлення вторгнень, підсистема, аналізатор, датчик, СВВ.

ВСТУП

Система виявлення вторгнень (СВВ) - програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу чи несанкціонованого управління ними. Схема розміщення СВВ у комп’ютерної мережі зображена на рисунку 1.

У сучасних системах виявлення виділяють наступні основні елементи: підсистему збору інформації, підсистему аналізу і модуль представлення даних.

- Підсистема збору інформації використовується для збору первинної інформації про роботу системи, яка захищається.
- Підсистема аналізу (виявлення) здійснює пошук атак і вторгнень в систему, яка захищається.
- Підсистема представлення даних дозволяє користувачу СВВ стежити за станом системи, яка захищається.

Підсистема збору інформації збирає дані про роботу системи, яка захищається. Для вивчення мережевого трафіку та виклику тривоги, коли ваша мережа знаходиться під атакою, СВВ повинна контролювати мережу за допомогою датчиків. Кількість використовуваних датчиків різна і залежить від специфіки системи, яка захищається.

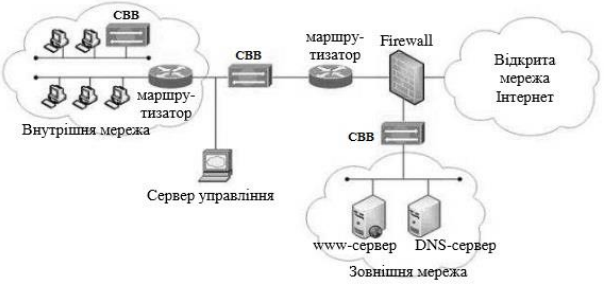

Рисунок 1. Схема розміщення СВВ у комп'ютерній мережі

Датчики в СВВ прийнято класифікувати за характером інформації, яка збирається. Відповідно із загальною структурою інформаційних систем виділяють такі типи:

- датчики додатків - дані про роботу програмного забезпечення системи, яка захищається;
- датчики хоста - функціонування робочої станції системи, яка захищається;
- датчики мережі - збір даних для оцінки мережевого трафіку;
- міжмережеві датчики - містять характеристики даних, що циркулюють між мережами.

Система виявлення вторгнення може включати будь-яку комбінацію з наведених типів датчиків.

Підсистема аналізу структурно складається з одного або більше модулів аналізу - аналізаторів. Наявність декількох аналізаторів потрібно для того, щоб підвищити ефективність виявлення. Кожен аналізатор виконує пошук атак або вторгнень певного типу. Вхідними даними для аналізатора є інформація з підсистеми збору інформації або від іншого аналізатора. Результат роботи підсистеми - індикація про стан системи, яка захищається. У разі, коли аналізатор повідомляє про виявлення несанкціонованих дій, на його виході може з'являтися деяка додаткова інформація. Зазвичай ця інформація містить висновки, що підтверджують факт наявності вторгнення або атаки.

Підсистема представлення даних необхідна для інформування зацікавлених осіб про стан системи, яка захищається. У деяких системах передбачається наявність груп користувачів, кожна з яких контролює певні підсистеми захищуємої системи. Тому в таких СВВ застосовується розмежування доступу, групові політики, повноваження і т.д.

ДОСЛІДЖЕННЯ

Щоб захистити мережу, СВВ повинна генерувати сигнали тривоги при виявленні підозрілої активності у мережі. Серед методів, що використовуються в підсистемі аналізу сучасних СВВ, можна виділити два напрями:

- виявлення аномалій.
- виявлення зловживань.

Кожен з цих напрямків має свої переваги і недоліки, тому в більшості існуючих СВВ застосовуються комбіновані рішення, засновані на синтезі відповідних методів. Ідея методів, що використовується для виявлення аномалій, полягає в тому, щоб розпізнати, чи є процес, що викликав зміни в роботі системи, діями зловмисника.

Розрізняють дві групи методів виявлення аномалій:

- з контрольованим навчанням.
- з неконтрольованим навчанням.

Для виявлення аномалій, необхідно створити профіль для кожної групи користувачів в системі. Ці профілі можуть бути побудовані автоматично або створені вручну. Ці профілі потім використовуються в якості основи для визначення нормальної активності користувачів. Якщо будь-яка мережева активність відхиляється занадто далеко від цієї базової лінії, то генерується сигнал тривоги.

Друга основна категорія СВВ відома як - виявлення зловживань. Виявлення зловживань також іноді називають сигнатурним детектуванням, тому тривоги генеруються на основі конкретних сигнатур атак. Ці атаки охоплюють певний тип трафіку або активності, заснований на відомій підозрілій діяльності.

Системи виявлення аномалій мають ряд переваг. По-перше, вони можуть дуже легко виявити крадіжку або інсайдерську атаку. Якщо реальний користувач або хтось, хто використовує викрадений аккаунт, починає виконувати дії, які знаходяться за межами нормального профілю користувача, генерується сигнал тривоги. По-друге, тому, що система заснована на профілях, дуже важко для атакуючого бути впевненим, що його дійльність залишиться непоміченою.

РЕКОМЕНДАЦІЇ

Розглянувши різні напрямки, шляхом об'єднання декількох методів в єдиний ми отримаємо - гібридну систему, яка має переваги декількох підходів, долаючи багато недоліків.

Об'єднання кількох різних напрямів СВВ в єдину систему, теоретично може виробляти набагато сильнішу СВВ. Різні напрями СВВ вивчають трафік і відшукують підозрілу діяльність по-різному. Основний недолік гібридної СВВ - чи сможуть, різні технології розпізнавання підозрілої діяльності, ефективно взаємодіяти між собою. Для отримання ефективної СВВ, необхідно правильно налаштувати СВВ, щоб не було конфліктів.

Подальші напрями вдосконалення пов'язані з впровадженням у теорію і практику СВВ загальної теорії систем, методів теорії синтезу та аналізу інформаційних систем і конкретного апарату теорії розпізнавання образів, так як ці розділи теорії дають конкретні методи дослідження для області систем СВВ.

У зв'язку з наявністю значної кількості факторів різної природи, функціонування інформаційної системи і СВВ має імовірнісний характер. Тому актуальним є обгрунтування виду імовірнісних законів конкретних параметрів функціонування.

ВИСНОВКИ

Система виявлення вторгнень – одна з найважливіших елементів системи інформаційної безпеки мережі будь-якого сучасного підприємства. На підприємствах (великих та малих) використовують, як стандартний метод захисту від крадіжки – систему сигналізації, і не приділяють значну увагу захисту інформації, яка циркулює в компьютерній мережі. Система виявлення вторгнень є, по суті, системою охоронної сигналізації для мережі підприємства. Вона дозволяє стежити за станом мережі для виявлення підозрілої діяльності. При виявленні підозрілої діяльності, СВВ генерує сигнал тривоги, щоб адміністратор знав, що мережа, можливо, під загрозою.

В практичній діяльності накопичений великий досвід вирішення проблем пов'язаних з виявленням вторгнень. Подальше вдосконалення СВВ пов'язано з конкретизацією методів синтезу та аналізу систем, теорії розпізнавання образів у застосуванні до СВВ. Для правильної та якісної роботи СВВ, необхідно ретельно налаштувати механізми захисту системи.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Партыка,Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.
2. Ярочкин, В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2008. - 544 с.
3. J. Allen, A. Christie, W. Fithen, J. McHuge, J. Pickel, E. Stoner, State of Practice of intrusion detection technologies // Technical Report CMU/SEI-99-TR-028. Carnegie Mellon Software Engineering Institute. 2000.
4. D. Denning, An Intrusion Detection Model. // IEEE Transactions on Software Engineering, v. SE-13, № I, 1987, pp. 222-232.

УДК 336.717.113

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ МАНІПУЛЮВАННЯ СВІДОМІСТЮ КЛІЄНТІВ БАНКУ ЯК ЗАГРОЗА ОТРИМАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Маслов Дмитро Миколайович, Мєшков Вадим Ігорович
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, Maslov_D@hotmail.com, local@i.ua

У тезисах проаналізована проблема банківського шахрайства. Розглянуті деякі прийоми маніпуляцій з використанням притаманним кожній людині психологічних особливостей. Розглянуті можливі наслідки та способи протидії цим маніпуляціям.

Ключові слова – шахрайство, банківська безпека, маніпуляція свідомістю, недобросовісна конкуренція, конфіденційна інформація.

ВСТУП

Системи захисту інформації в банківських системах невпинно розвиваються, впроваджуються нові технології аутентифікації, розроблюються нові більш безпечні протоколи обміну даними, використовуються більш криптостойкі ключі. Всі ці заходи направлені на забезпечення стабільності в роботі банку, безпеки даних клієнтів та їх особистих рахунків.

Але не варто забувати, що основним і найслабкішим місцем банківської системи залишається сама людина, а точніше клієнт. Вплив на цю ланку може дестабілізувати роботу банку і негативно позначитись на його репутації. Вплив на клієнтів банку може здійснюватися через маніпулювання свідомістю.

ІДЕЯ МАНІПУЛЯЦІЇ

Маніпуляція – це завуальований психологічний вплив на співрозмовника з метою досягнення вигідної для маніпулятора поведінки від нього.

Маніпулятори як правило використовують найбільш глибинні почуття людей серед яких: страх, надія, сором, тривога. Серед цього списку особливим чином слід виділити почуття страху, адже саме на ньому і ґрунтується більшість маніпуляцій. На сьогоднішні день більшість збережень знаходиться в банках, і клієнти бояться втратити ці заощадження, а в деяких випадках втратити все. Відчуття страху посилюється якщо є певна недостатність інформації, чим неодмінно теж користуються маніпулятори. Розглянемо деякі технології маніпуляцій, їх наслідки та протидія ним. В ролі маніпуляторів можуть виступати: банки конкуренти, спекулянти, шахраї.[1]

ЧУТКИ АБО НЕПРАВДИВА ІНФОРМАЦІЯ

ЗМІ та Інтернет займають велику частину інформаційного життя сучасної людини, саме з цих каналів ми отримуємо більшу частину інформації. З однієї сторони - постійно отримуємо нову інформації але, з іншою нам все важче стає відфільтрувати та оцінити те, що було почуто чи побачено.

Такий розвиток подій дає можливість провести маніпуляцій з використанням чуток та ефекту натовпу. Маніпулятор через ЗМІ чи Інтернет пускає неправдиву інформацію про стан банку і про те що треба негайно знімати всі вклади які зберігаються в цьому банку. Чи що у скорому часі зміниться курс певної валюти і треба негайно здати чи купити цю валюту. Негативний вплив такої маніпуляції, у тому що клієнти не маючи достовірної інформації по діяльності банку, його рахунків або котирування валюти, почнуть масово знімати вклади з втратою процентів, що не сумнівно негативно позначиться на економічному стані банку. Масовий обмін валют дасть додатковий прибуток спекулянтам які запустили цю недостовірну інформацію.

Також використовуються фіктивні записи розмов і транслюються як справжні. Або використовується фото-відео матеріалів у яких показується порожні банкомати чи відсутність готівки, що спонукає клієнтів зняти накопичення. Звичайно один клієнт не становить загрози стабільності банку але ж якщо таких клієнтів будуть сотні, банк понесе збитки.

Свою роль грає ефект натовпу: чим більше людей знімають гроші тим більший ажіотаж вони здійснюють, тоді банк йде на вимушені мірі такі як встановлення добового ліміту, що викликає певні незручності в першу чергу емоційні – начебто банк обмежує права клієнтів, що може негативно позначатися на його репутації.

Щоб не стати жертвою подібної маніпуляції слід тверезо оцінювати обставини, чітко розуміти звідки прийшла інформація і наскільки вона достовірна, хто її автор. Найпростіший метод – самостійна оцінка справ банку, для цього на сайті кожного банку міститься статистика діяльності банку, а також на сайті Національного банку України представленні данні фінансової звітності банків за поточний рік. Слід звертати увагу на оцінку експертів, але бути уважними та вибірковими, зважати на популярність експерта та його кваліфікаційний рівень.

У кожного великого банку є цілодобова гаряча лінія за якою можливо отримати всю інтересуючу інформацію. Найголовніше не піддаватися емоціям і, якщо це можливо, відкласти прийняття рішення і ще раз його обдумати в більш спокійній обстановці.[1-4]

СТРАХ, СПОДІВАННЯ ТА СОРОМ

На цих емоціях базуються шахрайські дії з банківськими картами клієнтів.

На відчутті сподівання базується одна з найпопулярніших махінацій, коли клієнту приходить повідомлення що він виграв цінний приз, і єдине що йому треба зробити це відправити данні карти для отримання виграшу, серед них можуть бути і секретні данні.

Також шахраї можуть використовувати відчуття страху у клієнтів, наприклад, коли клієнту телефонують і представляються співробітниками банку і повідомляють що рахунок був заблокований і найскоріше треба повідомити свій PIN, пароль чи підійти до банкомату та провести певні маніпуляції.

Звичайно у нормальному стані усі вище переліченні речі клієнт не стане робити, але гра іде на ефект раптовості, ейфорії, не залишаючи людині часу на роздуми.[1-4]

На відчутті сорому базується махінація яку як правило проводять в торгових центрах чи ресторанах. Коли клієнт розплачується банківською картою, не завжди до нього підходить працівник з POS-терміналом, і просить передати йому вашу карту. Клієнт соромиться виказати недовіру співробітнику і передає йому карту, а отже втрачає її з поля зору. Одразу гроші можуть не зникнути, але шахраю стануть відомі номер карти та CVV-код, а цього досить для здійснення Інтернет покупки.

Всі вищезазначені махінації ведуть до втрати коштів клієнтів. Щоб не стати жертвою шахраїв необхідно телефонувати в службу підтримки банку для уточнення стану рахунку, треба пам’ятати що безкоштовний сир лише в мишоловці і чітко розуміти які данні можна передавати третім особам, а які повинні бути в тайні. Слід завжди пам’ятати що всі поважають право на захист своєї інформації і немає нічого соромного в тому що ви бажаєте захищати свої особисті данні. У випадку ресторанна слід самостійно підійти до терміналу, але не втрачати карту с поля зору.

ВИСНОВКИ

Почуття людей залишаються їх слабким місцем, це використовують шахраї. Щоб не стати їх жертвою слід завжди тверезо оцінювати ситуацію не піддаватися емоціям, відкласти рішення на більш емоційно стабільний час. Банки підтримують безпеку клієнтів не тільки з технічного аспекту але з інформаційного: це повідомлення на сайті банку про популярні шахрайства, цілодобова гаряча лінія, SMS-оповіщення.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дашко Д. А., Мешков В. И. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ //Оргкомітет. – 2013. – С. 21.
2. Вільна енциклопедія Wikipedia «Манипуляция массовым сознанием» (Електроний ресурс) / Спосіб доступу: URL: http://ru.wikipedia.org/wiki/. – Загол.з екрана
3. Сайт НБУ (Електроний ресурс) / Спосіб доступу: URL: http://www.bank.gov.ua/– Загол.з екрана
4. Арансон Е., Пратканис Е. «Эпоха пропаганды: Механизмы убеждений, повседневное использование и злоупотребление». СПб.: прайм-ЕВРОЗНАК, 2003. – 384с.
5. Пресс-Служба ПриватБанка. (Електроний ресурс) / Спосіб доступу: URL: http://privatbank.ua/news/privatbank-rasskazal-o-5-tehnologijah-manipul-acii-soznanijem-klijentov/

УДК 65.012.8

ВНЕДРЕНИЕ НА ПРЕДПРИЯТИИ ПЛАНА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Смирнов Арсений Евгеньевич,
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, smirnov.a.e.work@gmail.com

В данной статье рассматриваются основные этапы плановых мероприятий при возникновении на предприятии инцидентов в сфере информационной безопасности. Перечислены главные цели, преследуемые при устранении последствий инцидента. Перечислен ряд методов достижения этих целей. Методика внедрения плана составлена исходя из исследований международных предприятий и организаций, специализирующихся на информационной безопасности бизнеса.

Ключевые слова – план реагирования, инцидент, кибер-угроза, информационная безопасность.

ВСТУПЛЕНИЕ

В условиях постоянного развития и создания новых угроз любое предприятие, даже при наличии систем защиты информации, рано или поздно сталкивается с инцидентами в сфере компьютерной и информационной безопасности. Установка одних только технических средств защиты и создание политик и процедур действий персонала при работе с информационными активами не является средством, гарантирующим абсолютную защищенность предприятия. В этой связи, крайне важным является наличие в компании внутреннего плана, определяющего регламент реагирования на компьютерные инциденты (cyber-incident).[1] Акцент в данном случае необходимо сделать на принятии рисков и максимально быстром реагировании на происшествия, с целью смягчения последствий. Следующие шаги предназначены для руководящего состава служб управления информационной безопасностью на предприятиях и способствуют эффективному реагированию на нарушения информационной безопасности.

ОСНОВНЫЕ ШАГИ СОЗДАНИЯ ПЛАНА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

1. Подготовка

Необходимо провести аудит конфиденциальной информации: выявить места её хранения и разработать стратегию защиты. Данные меры сократят временные затраты на установление нанесенного ущерба в случае атаки. Обследуемые данные должны включать в себя: информацию, идентифицирующую личность; данные кредитных карт; данные, составляющие коммерческую тайну интеллектуальную собственность; персональные данные.[1]

Крайне важным является непрерывное обучение. Группы реагирования всегда должны быть в состоянии готовности, обладать актуальными данными о расположении конфиденциальной информации, содержать систему в актуальном состоянии, проводить тестирование уязвимостей, совершенствовать процесс реагирования, проводя постоянные учения.

2. Обнаружение и выявление

Существует два способа эффективного выявления кибер-угроз: анализ безопасности конечных устройств и автоматизация:[2]

- Анализ безопасности конечных устройств: сбор информации со всех серверов и рабочих станций позволяет создать полную картину происходящего в информационной системе, что дает возможность обнаружить аномальное поведение, зоны риска и угрозы безопасности ещё до нанесения ущерба. Внедрение в информационную сеть систем обработки информационных событий (Security Information and Event Management (SIEM)) позволяет быстро обнаруживать угрозы в любой точке сети. Данные системы способны автоматизировать процесс обнаружения инцидентов с документированием в собственном журнале или внешней системе, а также своевременно информировать о событии. События должны не только собираться в хранилище для разбора по факту инцидента, но и обрабатываться. Инструменты SIEM позволяют сократить время, необходимое для разбора инцидента, своевременно обнаруживать, предотвращать угрозы и оперативно реагировать на них.[3]

3. Сортировка

После обнаружения угроз необходимо произвести их оценку, критичность и анализ текущих возможностей по её устранению. Наиболее угрозы должны быть нейтрализованы в первую очередь.

4. Оценка и локализация

В центре внимания на этом этапе должно быть сдерживание угрозы. Команда реагирования должна сосредоточить усилия на обработке вредоносных программ с помощью технических и программных средств. Основная цель заключается в устранении вредоносного программного обеспечения из сети. Угроза должна быть локализована, с целью определения характера её действий и выявления способа устранения.

5. Восстановление

После того, как установлено количество и характер атакуемых информационных активов, а угрозы обнаружены и идентифицированы, необходимо произвести восстановление безопасности системы. Группа реагирования должна произвести удаление всех вредоносных и несанкционированных программных средств. Одновременно с этим необходимо произвести аудит информационных активов системы, выявить пострадавшие от атаки устройства, чтобы удостовериться, что все данные находятся в защищенных разделах информационной системы.

После устранения инцидента необходимо продолжать наблюдение за системой для контроля восстановления после атаки до изначального, оптимального состояния.

6. Анализ последствий

Группа реагирования на инциденты должна провести анализ всех подразделений, задействованных в обработке информационных активов которые были подвержены атаке. Для пользователей этих подразделений должны быть составлены инструкции реагирования на данные инциденты. Пользователи иметь план, в соответствии с которым они смогут информировать службу безопасности предприятия о нарушениях информационной безопасности в установленном данной инструкцией порядке.[3]

Необходимо составить отчет по произошедшему инциденту, отражающий нанесенный ущерб, меры по противодействию угрозе и восстановлению, характере угрозы и мерах принятых для защиты от её реализации в будущем. Данный отчет имеет большое значение для всех заинтересованных сторон с точки зрения деловой репутации, конкурентоспособности, жизнеспособности предприятия, так как его содержание будет отражать способность предприятия противодействовать возникновению инцидентов в сфере информационной безопасности.[3]

ГРУППА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

Группа реагирования на инциденты — это группа специалистов, готовых быстро реагировать на угрозы информационной безопасности предприятия. Соответствие персонала определяется техническим опытом, его размещением, доступностью и готовностью в чрезвычайной ситуации принять соответствующие меры по защите информационных активов предприятия.

Группы реагирования состоят из системных и сетевых администраторов, а также экспертов по информационной безопасности. Системные администраторы отвечают за использование системных ресурсов, в том числе резервного копирования данных, имеющегося запасного оборудования и т.д. Сетевые администраторы осуществляют контроль сетевых протоколов и маршрутизации сетевого трафика. Задача специалистов по информационной безопасности отследить и очертить возникшие проблемы безопасности, а также провести анализ скомпрометированных систем после атаки. [2]

ЗАКЛЮЧЕНИЕ

Наличие четких рекомендаций и правил для сотрудников служб защиты информации, в случае возникновения инцидентов в сфере информационной безопасности, позволит не только в максимально короткие сроки восстановить работоспособность системы, но также существенно облегчить процедуру расследования и анализа инцидента для предотвращения подобных случаев в будущем.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Международный стандарт ИСО/МЭК 27001 Первое издание 2005-10-15 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования

2. Совместное исследование ЗАО «Лаборатория Касперского» и B2B International "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА 2013"

3. Отчет «HP 2013 cyber risk report» Hewlett-Packard Development Company, L.P.

УДК 004.056

ОСНОВНЫЕ ПРОБЛЕМЫ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕСА ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ УСТРОЙСТВ

Смирнов Арсений Евгеньевич,

ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, smirnov.a.e.work@gmail.com

В данной статье рассматриваются основные аспекты использования мобильных устройств (планшетов и смартфонов) – корпоративных и личных для доступа к информационным ресурсам предприятия, в контексте обеспечения информационной безопасности. Приведены основные современные методы снижения рисков при их испоьзовании.

Ключевые слова – мобильные устройства, конфиденциальная информация, информационная безопасность.

ВСТУПЛЕНИЕ

За последние годы использование мобильных устройств в корпоративной среде набирает всё большую популярность. Количество мобильных устройств, эксплуатируемых работниками различных организаций, возросло многократно. Активное развитие в течение последних нескольких лет получила концепция использования личных мобильных устройств сотрудников в рабочих целях, получившая в англоязычной среде название BYOD (Bring Your Own Device). Современный бизнес поощряет мобильность сотрудников, делая их более лояльными, позволяя находиться вне офиса и выполнять рабочие задачи. По оценкам Gartner, количество мобильных устройств, используемых в корпоративной среде, непрерывно увеличивается, и по прогнозам к 2015 году соотношение стационарных рабочих станций и мобильных устройств в корпоративной среде станет почти равным.[1]

Использование собственных устройств порождает дополнительные IT-риски для компаний, так как новые устройства превращаются в точки доступа к корпоративной инфраструктуре.

ОСНОВНЫЕ УГРОЗЫ ПРИ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ УСТОЙСТВ

В условиях все большего вовлечения мобильных устройств в корпоративную среду организаций

управление ими становится приоритетной задачей. Основной причиной развития данной технологии для пользователей в первую очередь служит возможность удаленного, мобильного доступа к корпоративным информационным ресурсам организации. Стремление руководства удовлетворить данную потребность своих сотрудников порождает ряд проблем с точки зрения информационной безопасности. Мобильные устройства сотрудника обычно используются в местах, не контролируемых компанией, и даже если устройства используются внутри офиса, они переносятся с места на место, что создает угрозу утечки конфиденциальных данных. Смартфоны и планшеты могут быть потеряны или украдены, и данные, хранимые на них, подвергаются риску быть скомпрометированными. Устройства могут попасть в руки злоумышленников, которые попытаются получить конфиденциальные данные либо напрямую с устройства, либо используя их для удаленного доступа к ресурсам организации. Совокупность этих и других обстоятельств порождает четыре основных угрозы, имеющих разные варианты реализации:[2]

- нарушение конфиденциальности информации в результате кражи или утери устройства;
- нарушение конфиденциальности информации в результате доступа посторонних лиц к устройству, оставленному без присмотра;
- доступ к конфиденциальной информации внешних нарушителей посредством использования вредоносного программного кода;
- хищение информации работником, имеющим легитимный доступ к информации и хранящий эту информацию на своем устройстве (путем отправки через личную почту, выкладывания в облачных сервисах хранения данных и проч.).[2]

МЕТОДЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ

Учитывая выше описанные проблемы для обеспечения информационной безопасности на предприятии, приоритетным является решение следующих задач:

- разработка политик управления мобильными устройствами, как выдаваемыми своим сотрудникам самими организациями, так и приобретаемыми сотрудниками самостоятельно на свои средства;
- обеспечение соблюдения политик и регламентов использования этих устройств, предоставление доступа, развертывание и обновление приложений;
- обеспечение соблюдения политик и регламентов использования мобильных устройств с технической точки зрения;
- оказание дальнейшей поддержки пользователям.[3]

Составной частью стратегии обеспечения безопасности конфиденциальной информации при использовании мобильных устройств внутри корпоративной сети является внедрение системы управления мобильными устройствами. Данный метод заключается в том, что на предприятии устанавливается один или несколько серверов, обеспечивающих централизованное управление, а на все мобильные устройства устанавливаются клиенты, которые настраиваются для постоянной работы в фоновом режиме. Если устройство выдано организацией, клиентское приложение управляет конфигурацией и безопасностью всего устройства (режим управления мобильными устройствами, MDM). Если устройство принадлежит сотруднику, то клиентское приложение управляет только конфигурацией и безопасностью самого приложения и корпоративных данных (режим управления мобильными приложениями, MAM). Клиентское приложение и корпоративные данные изолированы от прочих приложений и данных устройства, помогая сохранить конфиденциальность, как корпоративных данных, так и личного контента пользователя.[3]

Однако другая, наиболее серьезная угроза состоит в том, что, как правило, у организаций нет возможности контролировать безопасность сетей, используемых мобильными устройствами. Системы связи поддаются прослушиванию, что может привести к компрометации передаваемых данных. Атаки типа «человек посередине» также могут использоваться для перехвата и изменения соединения. Организации должны придерживаться презумпции небезопасности соединения между мобильными устройствами и корпоративными ресурсами, если нет полной уверенности в том, что устройства будут использоваться только в контролируемых организацией сетях. Риски использования небезопасных сетей могут быть сокращены путем применения сложных алгоритмов шифрования для защиты конфиденциальности и целостности передаваемых данных, а также за счет взаимной аутентификации для проверки обоих узлов перед передачей данных.

ЗАКЛЮЧЕНИЕ

Использование вышеперечисленных методов позволяет в значительной степени сократить риски при использовании мобильных устройств. Однако на сегодняшний день, учитывая высокую скорость развития рынка смартфонов и планшетов, в корпоративной среде разработка общепринятой, надежной модели обеспечения информационной безопасности ещё не завершена. Наиболее важно в данном случае, чтобы организации придерживались презумпции ненадежности мобильных устройств и планировали предоставлять доступ к своим корпоративным данным и приложениями только при соблюдении всех необходимых мер обеспечения безопасности.[3]

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Gartner Forecast: Worldwide Business Use Smartphone 2010-2015 Forecast;
2. Годовой отчет Cisco по безопасности за 2013 год
3. NIST Special Publication 800-124 Revision 1 "Guidelines for Managing the Security of Mobile Devices in the Enterprise" - U.S. Department of Commerce National Institute of Standards and Technology

УДК 004.056.53

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ С ПОМОЩЬЮ DLP-СИСТЕМ

Гержан Сергей Геннадиевич, Масальская Елена Александровна
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, E-mail: 825800@mail.ru

В данной работе рассмотрены системы предотвращения утечки данных, их принцип работы, а также описаны основные преимущества данных систем в сравнении с остальными существующими средствами предотвращения утечек.

Ключевые слова – DLP-система, предотвращение утечки данных, безопасность информации.

ВВЕДЕНИЕ

Для борьбы с утечками данных используются различные средства защиты, однако, наибольшее развитие в последнее время получила технология DLP (Data Leakage Prevention – предотвращение утечки данных). Основное назначение DLP – обеспечивать защиту от случайного или намеренного распространения конфиденциальной информации со стороны сотрудников, имеющих доступ к информации в силу своих должностных обязанностей [1].

ЗАДАЧИ DLP-СИСТЕМ

Основными задачами систем защиты от утечек являются:

- получение описания защищаемых данных (настройка системы);
- распознавание защищаемых данных в потоке, исходящем из внутренней информационной сети компании вовне (распознавание действий, направленных на перемещение конфиденциальных данных);
- реагирование на обнаруженные попытки (формирование доказательной базы для расследования инцидентов) [2].

В первую очередь следует определить данные, перемещение которых будет контролироваться системой, "предъявить" их системе с использованием методов, описанных выше, и выявить ее реакцию на обнаруженные инциденты. Важны также и параметры реакции на инцидент – предполагает ли она блокирование какой-либо операции: отправка электронного письма, создание экранной копии защищаемого документа, запись данных на USB-накопитель. Независимо от блокирования, практически всегда в журнал системы заносится максимально подробная предметная информация об инциденте [3]. Необходимо также описать правила информирования об инциденте:

- сотрудника подразделения, отвечающего за обеспечение информационной безопасности;
- лица, являющегося владельцем информации;
- самого подозреваемого в попытке организации утечки.

В случае противодействия утечкам с использованием сетевого сценария, DLP-система позволяет осуществлять перехват (блокирование) или зеркалирование (только аудит) отправки, проводить анализ содержания отправки в соответствии с используемыми механизмами контроля (рис.1). Затем при обнаружении подозрительного содержания происходит информирование ответственного сотрудника, а детали инцидента заносятся в журнал системы. Отправка может быть приостановлена, если схема подключения DLP-модуля позволяет это сделать [4]. Большинство DLP-систем предполагает осуществление повторной доставки задержанных ранее сообщений. Назначенный сотрудник оценивает, насколько адекватным был вердикт системы и, если тревога оказывается ложной, вручную отдает команду провести отправку задержанного сообщения.

Рисунок 1. Механизм контроля

ОСОБЕННОСТИ DLP-СИСТЕМ

Основные практические достоинства DLP:

- способны классифицировать и выделять наиболее важные для защиты данные (развитые механизмы анализа содержимого);
- приспособлены для тотального охвата информационных потоков организации (множество отслеживаемых каналов, развитая система обработки инцидентов, гибкое распределение ролей);

подстраиваются под существующие бизнес-процессы (эффект от использования DLP достижим без организационных преобразований и увеличения штата). Система DLP будет просматривать все информационные потоки и информацию, выводимую на сменные устройства записи, будет обнаруживать конфиденциальные данные в потоках и активно реагировать на обнаруженные попытки распространения конфиденциальной информации

Основные недостатки DLP-систем:

- не содержат встроенных средств шифрования;
- методы классификации данных, используемые в DLP и подходящие для глобального охвата всех обрабатываемых ресурсов, могут пропустить те данные, которым система не была обучена.

ВЫВОДЫ

Применение DLP-систем рекомендуется для организаций, которые ведут активный обмен документами с внешними контрагентами, а при этом стоит задача обеспечения конфиденциальности этого процесса. Например, из медицинского учреждения не сможет беспрепятственно произойти утечка историй болезней сразу сотни человек частному лицу, из банка – баз кредитных карт и персональных данных клиентов. По результатам перемещений конфиденциальных данных ведется подробная статистика с возможностью отслеживания соответствия требованиям действующих стандартов безопасности. Для повышения эффективности работы системы следует совместить использование в едином программном комплексе, методов DLP и шифрования данных, а также адаптировать методы обучение системы.

Обучение системы осуществляется:

- вводом образцов конфиденциальной информации, разбитой по категориям (обычно организация указывает, в каких рабочих папках на серверах находятся массивы документов) для снятия цифровых отпечатков;
- вводом выгрузок из актуальных баз данных для снятия отпечатков баз данных;
- включением существующих заведенных в системе шаблонов политик обнаружения (например, номеров кредитных карт, номеров российских паспортов, ключей активации программных продуктов, реагирования на отправку зашифрованных вложений);
- вводом собственных слов и выражений, характерных для конфиденциальных данных;
- вводом исключений (например, шаблоны договоров).

Объединение методов шифрование и DLP-систем позволяет контролировать информацию, покидающую пределы корпоративной сети, защитить серверные хранилища и съемные носители, которые физически могут попасть в руки посторонних лиц. Таким образом, шифрование может существенно расширить возможности DLP-систем и снизить риски утечки конфиденциальных данных.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Предотвращение утечек информации (Электрон. ресурс) / Способ доступа: URL: http://ru.wikipedia.org/wiki/dlp
2. Как работают DLP-системы: разбираемся в технологиях предотвращения утечки информации (Электрон. ресурс) / Способ доступа: URL: http://www.xakep.ru/post/55604/
3. DLP-Lite (Электрон. ресурс) / Способ доступа: URL: http://habrahabr.ru/post/150227/
4. Обзор DLP систем (Электрон. ресурс) / Способ доступа: URL: http://www.itsec.ru/articles2/techobzor/obzor-sistem-dlp-v-chem-raznica

УДК 004.056

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ МНОГОПОТОЧНЫХ ТЕХНОЛОГИЙ В РЕАЛИЗАЦИИ СЕТЕВЫХ СКАНЕРОВ БЕЗОПАСНОСТИ

Емельченко Е.Е., Тимофеев Д.С.

Государственное ВУЗ «Национальный горный университет», http://bit.nmu.org.ua/

В данной статье рассматривается эффективность разработки сетевых сканеров безопасности с использованием многопоточных технологий.

Ключевые слова – информационная безопасность; уязвимость; многопоточность; сетевой сканер.

ВВЕДЕНИЕ

С расширением использования корпоративных сетей и сети Internet, профессионалы в области защиты сетей и информационных систем все больше осознают необходимость анализа и управления потенциальными рисками безопасности в своих сетях и системах. Анализ уязвимостей – это процесс обнаружения, оценки и ранжирования этих рисков, связанных с системами и устройствами, функционирующими на сетевом и системном уровнях, с целью рационального планирования применения информационных технологий. Инструменты, реализующие этот процесс, позволяют установить собственную политику безопасности, автоматизировать анализ уязвимостей и создать отчеты, которые эффективно связывают информацию об обнаруженных уязвимостях с подробными корректирующими действиями на всех уровнях организации. Одновременное использование систем анализа защищенности, функционирующих на сетевом и системном уровнях, обеспечивает мощнейшую защиту против трех типов уязвимостей, вводимых поставщиком, администратором и пользователем [1].

РИСКИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Все риски можно разделить на три категории:

1. Риски, связанные с ПО, поставляемым поставщиком – включает ошибки, неустановленные обновления операционной системы, уязвимые сервисы и незащищенные конфигурации по умолчанию.

2. Риски, связанные с действиями администратора – включает доступные, но не правильно используемые настройки и функции системы, не отвечающие политике безопасности требования к минимальной длине пароля и

несанкционированные изменения в конфигурации системы.

3. Риски, связанные с деятельностью пользователя – включают уклонение от предписаний принятой политики безопасности, например, отказ запускать ПО для сканирования вирусов или использование модемов для выхода в сеть Интернет в обход межсетевых экранов и другие, более враждебные действия.

АКТУАЛЬНОСТЬ МНОГОПОТОЧНОСТИ

Но, к сожалению, до сих пор мышление многих программистов при разработке программ остается чисто последовательным. Не учитываются широкие возможности параллелизма, в частности, многопоточности. Многопоточность имеет большие преимущества:

- Увеличение скорости (по сравнению с использованием обычных процессов). Многопоточность основана на использовании облегченных процессов, работающих в общем пространстве виртуальной памяти. Благодаря многопоточности, не возникает больше неэффективных ситуаций, типичных для классической системе UNIX, в которой каждая команда shell (даже команда вывода содержимого текущей директории ls исполнялась как отдельный процесс, причем в своем собственном адресном пространстве. В противоположность облегченным процессам, обычные процессы (имеющие собственное адресное пространство) часть называют тяжеловесными.
- Использование общих ресурсов. Потоки одного процесса используют общую память и файлы.
- Экономия. Благодаря многопоточности, достигается значительная экономия памяти, по причинам, объясненным выше. Также достигается и экономия времени, так как переключение контекста на облегченный процесс, для которого требуется только сменить стек и восстановить значения регистров, значительно быстрее, чем на обычный процесс [3].

ИСПОЛЬЗОВАНИЕ МНОГОПОТОЧНОСТИ В СЕТЕВЫХ СКАНЕРАХ БЕЗОПАСНОСТИ

Использование мноопоточности при разработке сетевого сканера позволяет увеличить эффективность таких его функций:

1. Сканирование сети

- Сканирование IP-адресов. Как правило, речь идет о рассылке широковещательных пакетов ICMP. Утилиты отправляют пакеты типа ICMP ECHO по указанному IP-адресу и ожидают ответного пакета ICMP ECHO_REPLY. Получение такого пакета означает, что в данный момент компьютер подключен к сети по указанному IP-адресу.
- Сканирование портов. Механизм сканирования портов основан на попытке пробного подключения к портам TCP и UDP исследуемого компьютера с целью определения запущенных служб и соответствующих им портов. Обслуживаемые порты могут находиться в открытом состоянии или в режиме ожидания запроса. Определение портов, находящихся в режиме ожидания, позволяет выяснить тип используемой операционной системы, а также запущенные на компьютере приложения.

2. Локальный аудит паролей

- Взлом словарём. Алгоритм основан на предположении, что в пароле используются существующие слова какого-либо языка, либо их сочетания, т.е. существует файл с набором слов, которые могут считаться наиболее вероятно используемыми в качестве взламываемого пароля.
- Взлом полным перебором. Алгоритм решения задачи заключается в переборе всех возможных вариантов паролей. Сложность полного перебора зависит от количества всех возможных решений задачи. Если пространство решений очень велико, то полный перебор может не дать результатов в течение нескольких лет или даже столетий. Любая задача может быть решена полным перебором, но следует помнить, что, в зависимости от количества всех возможных решений полный перебор может потребовать экспоненциального времени работы.

3. Сетевой аудит паролей. Средство сетевого аудита паролей предназначено для удаленного поиска и выявления паролей, содержащих легко подбираемые символьные комбинации. Сетевой аудит основан на взломе паролей через словарь с использованием соответствующих сетевых протоколов.

4. Системный аудитор. Системный аудитор предназначен для сканирования рабочей станции на предмет определения параметров установленных операционных систем, системных, коммуникационных и периферийных устройств, в том числе USB-устройств.

5. Средство поиска по диску. Средство поиска по диску предназначено для поиска информации по ключевым словам на носителях данных (жестких дисках, дискетах, оптических дисках)[2].

ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ

1. Руководство по выбору технологии анализа защищенности (Електрон. ресурс) / Способ доступа: URL: http://kiev-security.org.ua/box/12/74.shtml.

2. Закрытое акционерное общество научно-производственное объединение «Эшелон». Программный комплекс «Средство анализа защищенности Сканер ВС». Описание программы. / Способ доступа: URL: http://scaner-vs.ru/data/description_sca.pdf.

3. Интуит. Основы современных операционных систем. Лекция 10: Потоки и многопоточное выполнение программ (Електрон. ресурс) / Способ доступа: URL: http://intuit.ru/studies/courses/641/497/lecture/11284.

УДК 004.056

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОНТЕНТУ ЦИФРОВОГО МОВЛЕННЯ ПРИ РЕАЛІЗАЦІЇ IPTV ТЕХНОЛОГІЇ

Прокопчук Олександр Євгенович
Науковий керівник: ст. викл. Святошенко В.О.
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, alex0392@gmail.com

Аналіз існуючих систем захисту цифрового контенту. Розробка рекомендацій щодо посилення рівня безпеки IPTV технології, та захисту від зловмисників.

Ключові слова – IPTV технологія, безпека контенту, цифрове мовлення.

ВСТУП

У наш час багато хто замінює звичайний телевізор на комп'ютер або взагалі не має телевізору. Усі користувачі ПК переглядають телебачення по технології IPTV (англ. Internet Protocol Television).

Технологія IPTV – цифрове інтерактивне телебачення в мережах передачі даних за протоколом IP, нове покоління телебачення.

Архітектура комплексу IPTV як правило включає в себе такі компоненти:

- підсистема управління комплексом та послугами, яку ще називають «Проміжне програмне забезпечення» або «IPTV Middleware»;
- підсистема прийому та обробки контенту;
- підсистема захисту контенту;
- підсистема відео серверів;
- підсистема моніторингу якості потоків та клієнтського обладнання.

Доставка контенту до клієнтського обладнання здійснюється поверх IP-мережі оператора.

Головними перевагами IPTV є інтерактивність відеопослуг і наявність широкого набору додаткових сервісів:

- відео на вимогу;
- зсув по часу;
- персональна мережа відеозапису.

Можливості протоколу IP дозволяють надавати не тільки відеопослуги, але й набагато ширший пакет послуг, в тому числі інтерактивних та інтегрованих.

Крім основних послуг IPTV може включати в базовий пакет ряд додаткових сервісів:

1. відео-телефон;
2. голосування;
3. інформаційній портал;
4. ігри.

Це можливо на основі уніфікації і стандартизації різних кінцевих пристроїв, інтеграції звуку, відео і даних на основі IP-протоколу та надання послуг на єдиній технологічній платформі.

В IPTV є можливість використовувати для одного відеоряду два і більше каналів звукового супроводу, наприклад українською та англійською мовами, самі канали при цьому можуть бути поліфонічними.

Перевага IPTV перед кабельним та супутниковим ТБ:

- нема потреби в придбанні додаткового дорогого обладнання;
- не потрібно встановлювати обладнання;
- зображення DVD якості, стереозвук;
- можливість запису потокового відео на ПК користувача;
- інноваційна послуга за доступною ціною.

ДОСЛІДЖЕННЯ

Основні проблеми при трансляції за допомогою технології IPTV:

- ймовірна компрометація контенту;
- ретрансляція сигналу далі, без відома Інтернет-провайдера.

Щоб уникнути несакціонованного розповсюдження інформації – потрібно запобігти ретрансляції контенту іншому користувачеві.

Зловмисник або недобросовісний клієнт може підмінити контент або ретранслювати іншим особам відповідно.

На рисунку 1 зображено, як контент передається до користувача.

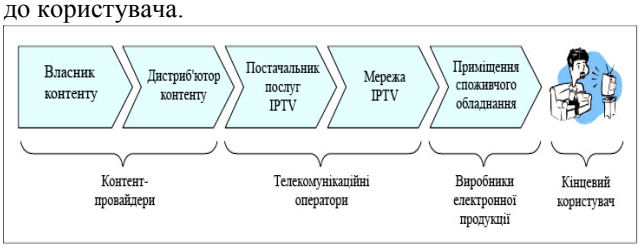

Рисунок 1. Передача контенту до користувача

За умовами договору багатьох провайдерів IPTV, ретранслювати сигнал заборонено, тому вони мають право відключити клієнта від мережі Інтернет.

Як відомо, інформація, яка передається користувачу має такі властивості:

1. конфіденційність;
2. цілісність;
3. доступність.

Однак, у мережі IPTV недостатньо забезпечується цілісність тому, що існують такі загрози:

Клієнтська інформація. Зловмисники можуть змінювати записи або інформацію клієнта, наприклад, шляхом додавання або видалення платежів на рахунок або наданих послуг.

Зміст інформації. Простим прикладом є потенційна модифікація контенту. Наприклад, зловмисники можуть маніпулювати вихідним контентом і вставляти аморальну, політичну чи інші комерційну інформацію в трансляції. В результаті отримаємо контент з рекламними вставками від зловмисників.

РЕКОМЕНДАЦІЇ

Для нового покоління телевізорів ця проблема частково вирішена, але в наш час більше людей користуються комп'ютерами.

Для телевізорів існує декілька систем захисту контенту:

1. використання смарт-карт для контролю доступу;
2. шифрування аудіо- та відео контенту;
3. авторизація абонентів.

Але це не дає стовідсоткову гарантію захисту. З розвитком технології – потрібно удосконалювати системи захисту.

У випадку з комп'ютером можна удосконалити програми перегляду IPTV додавши до них індивідуальні сертифікати з індивідуальними мітками. Кожен провайдер компілює програму перегляду для усіх клієнтів, згодом у кожного клієнта в Особистому Кабінеті провайдера потрібно скачати сертифікат, який додається до програми. Без цього сертифікату не буде йти сигнал, але якщо клієнт усе зробить правильно – перегляд буде захищеним. За допомогою такої системи досягається контроль цілісності пакетів.

ВИСНОВКИ

Сьогодні існує великий вибір операторів даної технології. У кожного з операторів існує своя система захисту, які відрізнятися алгоритмами шифрування контенту, способами передачі контрольного слова, застосовуваними апаратними та програмними засобами. Оператори технологій вкладають значні капіталовкладення на захист контенту. Однак у зв'язку з розвитком самої технології IPTV виникає і необхідність вдосконалення системи безпеки, використовуючи і вдосконалюючи всі перераховані вище компоненти захисту.

ПЕРЕЛІК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. IPTV (Електрон. ресурс) / Спосіб доступу: URL: http://ru.wikipedia.org/wiki/IPTV - Загол. з екрану
2. David H. Ramirez. IPTV Security: Protecting High-Value Digital Contents 2008
3. Защита контента IPTV-технологий (Електрон. ресурс) / Спосіб доступу: URL: http://www.rusnauka.com/16_NPRT_2009/Informatica/47241.doc.htm - Загол. з екрану
4. IPTV и спутниковое ТВ (Електрон. ресурс) / Спосіб доступу: URL: http://ubr.ua/expert-question/233 - Загол. з екрану
5. В помощь IP-телевизионщику (Електрон. ресурс) / Спосіб доступу: URL: http://www.connect.ru/article.asp?id=6039 – Загол. з екрану

УДК 65.012.8

РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ТЕОРЕТИКО-ІГРОВОЇ МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Бурцева Катерина Анатоліївна, проф., канд. физ.-мат. наук Сушко Світлана Олександрівна,
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, elvierace@rambler.ru

Розглядається процес розробки політики безпеки на основі аналізу ризиків при застосуванні теоретико-ігрової моделі інформаційної безпеки.

Ключові слова – політика безпеки інформації підприємства, інформаційна безпека підприємства, теорія ігор, аналіз ризиків, порушник, власник системи.

ВСТУП

Значну роль в процесі забезпечення інформаційної безпеки підприємства відіграють організаційні заходи: вони становлять близько 60% від усього комплексу заходів [1].

В основі організаційних заходів захисту інформації лежить політика безпеки (ПБ) інформації підприємства: від її ефективності залежить успішність забезпечення ІБ. У сучасній практиці забезпечення ІБ, термін «політика безпеки» може вживатися як у широкому, так і у вузькому змісті. У широкому змісті, ПБ визначається як система документованих управлінських рішень щодо забезпечення ІБ організації[2]. У вузькому змісті, під політикою безпеки інформації розуміють сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації[3]. Основною метою ПБ згідно з ISO 27000 [4] є забезпечення спрямування і підтримки інформаційної безпеки керівництвом. Згідно з цим стандартом даний документ (ПБ) повинен включати в себе наступне:

- визначення інформаційної безпеки, її загальні цілі та область дії
- заяву про наміри керівництва, що висвітлює цілі та принципи управління інформаційною безпекою;
- короткий опис політики безпеки, принципів, стандартів і нормативних вимог;
- визначення загальних і приватних обов'язків з управління інформаційною безпекою;
- посилання на документацію, яка може доповнювати опис політики.

АНАЛІЗ РИЗИКІВ І ТЕОРІЯ ІГОР

Для створення оптимальної політики безпеки інформації доцільно застосовувати процес аналізу ризиків. Він дозволить виявити найбільш критичні загрози та ризики, що вони спричиняють, та обрати оптимальну стратегію поведінки власника системи, на основі якої і буде побудована політика інформаційної безпеки підприємства. Для останнього і застосовується теоретико-ігрова модель інформаційної безпеки. Вона являє собою матрицю, в основі якої лежать стратегії поведінки власника системи і порушника (найбільш високі ризики). В загальному випадку вона має наступний вигляд:

$$H_{m\times n}=\begin{bmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ \dots & \dots & \dots & \dots \\ h_{m1} & h_{m2} & \dots & h_{mn} \end{bmatrix},$$

де *m*— кількість стратегій гравця 1(порушник);*n*— кількість стратегій гравця 2 (власник системи);*H*(*i, j*)— виграш гравця 1 в *ij*-ситуації[5].

В процесі аналізу ризиків необхідно обрати оптимальну стратегію гравця 2(власника системи), тобто зробити вибір між прийняттям, зниженням та передаванням ризику. Так, за допомогою теорії ігор ми розраховуємо частоту вірогідності вибору стратегії, розв´язавши систему нерівностей, яка створена на основі матриці і в загальному випадку має вигляд:

$$\left.\begin{array}{l} c_1y_1+(r_{21}+c_1)y_2+....+(r_{n1}+c_1)y_n\ge\upsilon \\ (r_{12}+c_2)y_1+...+c_2y_2+...+(r_{n2}+c_2)y_n\ge\upsilon \\ \dots \\ (r_{1n}+c_n)y_1+(r_{2n}+c_n)y_2+....+c_ny_n\ge\upsilon \end{array}\right\}.$$

де y1, y2 ,....., yn — частота ймовірностей щодо вибору стратегій гравцем 2 у побудові своєї змішаної стратегії, а Cj> 0 — витрати на захист від j-тої загрози;

rij > 0 — збиток у результаті реалізації j-тої загрози[6].

Для знаходження розв´язку даної системи треба мати наступні дані:

1. Можливі дії порушника (гравця 1) при виникненні вразливості на підприємстві(поява ризику) і дії власника системи.
2. Витрати на захист від j-тої загрози.
3. Збиток у результаті реалізації j-тої загрози.
4. Виграш гравця 2 в *ij*-ситуації.
5. Визначити ціну гри.

Розв’язавши систему ми обираємо оптимальну стратегію, яку перевіряємо за допомогою критерія Вальда, Севіджа, Байеса та інших, які діють в умовах ризику.

ВИСНОВОК

Для підвищення ефективності політики безпеки інформації треба орієнтуватися на обрану стратегію: це забезпечить мінімізацію можливих ризиків, а значить покращить стан інформаційної безпеки підприємства.

Теорія ігор,на відміну від статистики та експертних методів, дозволяє математично підтвердити обрану стратегію поведінки і оптимізувати процес розробки політики безпеки інформації, саме тому її доцільно застосовувати на практиці.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Выработка официальной политики предприятия в области информационной безопасности. Спосіб доступу:URL:http://unix1.jinr.ru/faq_guide /security/ jet/secplant/razd2.html – Загол. з екрану.
2. НД ТЗІ 1.4-001-2000. Спосіб доступу: URL: http://www.am-soft.ua/files/KSZI/1.4-001-00.pdf– Загол. з екрану.
3. НДТЗІ 1.1-003-99 Спосіб доступу: URL: http://info-stand.com/downloads/nd-tzi/1-1_003_99/NDTZI_1.1_003_99.pdf – Загол. з екрану.
4. ISO 27000. Спосіб доступу: URL: http://niisokb.ru/news/documents/IDT%20ISO%20IEC%2027000-2011-09-14.pd– Загол. з екрану.
5. Шиян А.А. Теорія ігор: основи та застосування в економіці та менеджменті / Спосіб доступу: URL: http://inrtzp.vntu.edu.ua/pmba/stf/teach/books/Theory.pdf – Загол. з екрану.
6. Тынкевич М.А ЭЛЕМЕНТЫ ТЕОРИИ ИГР И СТАТИСТИЧЕСКИХ РЕШЕНИЙ / Спосіб доступу: URL: http://vtit.kuzstu.ru/books/shelf/book1/index.html – Загол. з екрану.

УДК 65.012.8

ЗАСТОСУВАННЯ SWOT-АНАЛІЗУ В ПРОЦЕСІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Буднік Марина Миколаївна, проф., канд. физ.-мат. наук Сушко Світлана Олександрівна
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, Marina_Dnepr17@mail.ru

Розглядається SWOT-аналіз і можливість його застосування в процесі управління ризиками інформаційної безпеки. Наводиться приклад матриці SWOT, матриці можливостей та загроз. Робляться висновки, щодо ефективності SWOT-аналізу.

Ключові слова: управління ризиками, інформаційна безпека, загрози, SWOT-аналіз.

ВСТУП

У наш час управляти ризиками абсолютно необхідно не тільки для отримання конкурентних переваг, а й для виживання в цілому. Багато питань в галузі управління ризиками ІБ залишаються не до кінця дослідженими, крім того, рішення задачі управління ризиками ІБ ускладнюється через такі обставини, як нечіткість і якісність основних факторів ризику, необхідність прийняття рішень в умовах невизначеності та неповноти інформації. Таким чином, актуальним завданням стає розробка ефективного методу для вирішення задачі оцінки та управління ризиками інформаційної безпеки та його застосування на практиці.

SWOT-АНАЛІЗ

SWOT-аналіз─ метод стратегічного планування, розроблений Альбертом Хамфрі в 1960-х і 1970-х роках для різних маркетингових досліджень. Його механізм цілком універсальний, тому SWOT-аналіз широко розповсюджений і в інших областях.

Абревіатура SWOT складається з перших літер англійських слів: strengths─ сильні сторони, weaknesses ─ слабкості, opportunities ─ можливості, threats ─ загрози. Його можна використати або адаптувати для оцінки потенційних загроз, а слабкі сторони, про які йдеться в цьому аналізі, пов'язати з вразливостями в інформаційній безпеці. Цей аналіз має бути спрямований на конкретну мету, наприклад, на скорочення ризиків інформаційної безпеки або вироблення стратегії в інформаційній безпеці.

МАТРИЦЯ SWOT

Спочатку необхідно скласти список слабких і сильних сторін організації з урахуванням конкретної ситуації, в якій знаходиться організація, а також список загроз і можливостей. Після цього настає етап встановлення зв'язків між ними ─ складається матриця SWOT, зображена у таблиці 1. У рядках цієї таблиці виділяються сильні та слабкі сторони, виявлені на першому етапі аналізу організації, а у стовпцях матриці наводяться можливості та загрози організації [2]. На перетині розділів утворюється чотири поля: поле «СІМ» (сила і можливості), поле «СІЗ» (сила і загрози), поле «СЛМ» (слабкість і можливості), поле «СЛЗ» (слабкість і загрози). На кожному з даних полів потрібно розглянути всі можливі парні комбінації і виділити ті, що мають бути враховані при розробці стратегії поведінки організації.

Таблиця 1. Матриця SWOT

Можливості та загрози / Сильні, слабкі сторони організації	Можливості 1,2,3…	Загрози 1,2,3…
Сильні сторони 1,2,3…	ПОЛЕ «СІМ»	ПОЛЕ «СІЗ»
Слабкі сторони1,2,3…	ПОЛЕ «СЛМ»	ПОЛЕ «СЛЗ»

Для успішного застосування методології SWOT-аналізу організації важливо вміти не тільки розкрити загрози і можливості, але і спробувати оцінити їх з точки зору того, наскільки важливим для організації є врахування кожної з виявлених загроз і можливостей.

Для оцінки можливостей застосовується метод позиціонування кожної конкретної можливості у матриці можливостей (таблиця 2). Дана матриця будується наступним чином: у стовпцях відкладаються ступені впливу можливості на діяльність організації (сильний вплив, помірний вплив, малий вплив); у рядках наводиться ймовірність того, що організація зможе використати відповідну можливість (висока ймовірність, середня ймовірність, низька ймовірність). Отримані всередині матриці дев'ять полів можливостей мають різне значення для організації:

- можливості, які потрапляють на поля «ВС» (висока ймовірність і сильний вплив), «ВП» (висока ймовірність і помірний вплив), «СС» (середня ймовірність і сильний вплив), особливо важливі для організації і їх треба обов'язково використовувати;
- можливості, які потрапляють на поля «СМ» (середня ймовірність і малий вплив), «НП» (низька ймовірність і помірний вплив) і «НМ» (низька ймовірність і малий вплив), практично не заслуговують уваги організації;
- щодо можливостей, які потрапили на решту полів, керівництво має прийняти позитивне рішення про їх використання, якщо в організації достатньо ресурсів для цього.

Таблиця 2– Матриця можливостей

Ймовірність	Вплив можливості на діяльність організації		
	Сильний вплив	Помірний вплив	Малий вплив
Висока	ПОЛЕ «ВС»	ПОЛЕ «ВП»	ПОЛЕ «МВ»
Середня	ПОЛЕ «СС»	ПОЛЕ «СП»	ПОЛЕ «СМ»
Низька	ПОЛЕ «НС»	ПОЛЕ «НП»	ПОЛЕ «НМ»

Схожа матриця складається для оцінки загроз (таблиця 3).

Таблиця 3 – Матриця загроз

Ймовірність	Можливі наслідки для організації, до яких призводить реалізація загрози			
	Руйнування	Критичний стан	Тяжкий стан	Легкі пошкодження
Висока	ПОЛЕ «ВР»	ПОЛЕ «ВК»	ПОЛЕ «ВТ»	ПОЛЕ «ВЛ»
Середня	ПОЛЕ «СР»	ПОЛЕ «СК»	ПОЛЕ «СТ»	ПОЛЕ «СЛ»
Низька	ПОЛЕ «НР»	ПОЛЕ «НК»	ПОЛЕ «НТ»	ПОЛЕ «НЛ»

У першому стовпці записуються можливі наслідки для організації, до яких може призвести реалізація загрози (руйнування, критичний стан, важкий стан, легкі пошкодження), а у рядку наводяться ймовірність того, що загроза буде реалізована (висока ймовірність, середня ймовірність, низька ймовірність). Загрози, отримані всередині матриці, мають наступне значення для організації:

- загрози, які потрапляють на поля «ВР» (висока ймовірність і руйнування), «ВК» (висока ймовірність і критичний стан), «СР» (середня ймовірність і руйнування), дуже небезпечні для організації і вимагають негайного й обов'язкового усунення;
- загрози, що потрапили на поля «ВТ» (висока ймовірність і тяжкий стан), «СК» (середня ймовірність і критичний стан) і «НР» (низька ймовірність і руйнування), також повинні знаходитися в полі зору вищого керівництва і бути усунені в першочерговому порядку;
- щодо загроз, які знаходяться на полях «НК» (низька ймовірність та критичний стан), «СТ» (середня ймовірність і тяжкий стан) і «ВЛ» (висока ймовірність і легкі пошкодження), то керівництво має обрати уважний та відповідальний підхід до їх усунення;
- загрози, які попали у решту полів, теж потребують уваги. У цьому випадку має здійснюватися уважне відстеження їх розвитку, хоча при цьому не ставиться завдання їх першочергового усунення.

ВИСНОВОК

За результатами аналізу, по-перше, можна ідентифікувати внутрішні недоліки, що вимагають якнайшвидшого усунення, а по-друге, оцінити, чи володіє організація внутрішніми силами і ресурсами, щоб реалізувати наявні можливості і протистояти загрозам. Очевидно, методологія SWOT-аналізу стає

ефективною тоді, коли вдається не тільки розкрити загрози й можливості, а й врахувати ці два розділи аналізу в стратегії поведінки організації при управлінні ризиками інформаційної безпеки.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Chestnut D. Security SWOT Analysis. (Electronic resource) / Method of access URL: http://www.ehow.com/about_6654114_security-swot-analysis.html.

2. Воронина В.М., Кокарев Д.В. SWOT-анализ как современный инструмент исследования в целях антикризисного управления предприятием// Ежемесячный аналитический журнал «Слияния и Поглощения», 2007 г. - №3 (49). – с. 23-26.

3. Syed Majid Ali Shah Bukhari, InayatUllah Khan. SWOT Analysis of IP Multimedia Sub System Security Authentication Schemes,Blekinge, 2009.– p.1-48.

УДК 004.056

МЕТОДЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Романенко Екатерина Александровна, Тимофеев Дмитрий Сергеевич
ГВУЗ «Национальный горный университет» http://bit.nmu.org.ua/, re5565593@mail.ru

В данной работе представлены методы оценки эффективности систем управления информационной безопасности. Основной целью данной работы является раскрытие основных принципов оценки эффективности систем управления информационной безопасностью. так же раскрыта проблематика оценки эффективности систем управления информационной безопасностью.

Ключевые слова – система управления информационной безопасностью; оценка эффективности; метрики; информационная безопасность; информационные технологии.

ВСТУПЛЕНИЕ

На данном этапе развития информационных технологий (ИТ) все чаще возникает вопрос на сколько эффективны те или иные процессы информационной безопасности (ИБ). Решение данной проблемы наталкивает специалистов в ИБ на более глубокое изучение и анализ систем управления информационной безопасностью (СУИБ). Проанализировав СУИБ мы можем получить отчет который нам раскроет то на чем мы сможем снизить затраты в области ИБ, на какие аспекты нам стоит заострить внимание, и то на сколько эффективна наша СУИБ.

МЕТРИКИ ИБ И ОЦЕНКА ЭФФЕКТИВНОСТИ

Процедуры обеспечения ИБ реализуются различными механизмами. В процессе оценки эффективности необходимо выявить, насколько правильно они функционируют. Метрики оценки эффективности доступны для расчета и анализа, имеют количественное выражение (деньги, время, и т.д.). [1]

Хорошая метрика:

1. воспроизводима;
2. не содержит субъективных оценок;
3. проста в сборе данных;
4. выражается в числовых значениях;
5. отражает минимум одну сущность измерения;
6. понятна.

Описание метрики:

1. название метрики;
2. цель метрики;
3. источник данных, способ снятия;
4. частота снятия;
5. формула расчета;
6. подтверждение внедрения.[2]

Определив и сформулировав необходимые метрики, необходимо периодическое оценивание и вычисление метрик, для этого необходимо собрать большое количество исходной информации, которая хранится в различных местах: в базах данных, с логах систем, в отчетах подразделений и т.д. для сбора этих данных и их обработки можно использовать средства автоматизации, однако нужно аккуратно подходить к их выбору четко понимая какие данные и в каком количестве нам необходимы для качественного расчета.

После сбора данных необходимо провести их анализ. Анализ позволит нам ответить на вопросы: позволяют ли используемые средства обеспечения ИБ достичь поставленных целей? какими ресурсами можно достичь желаемого результата? можно ли использовать компенсирующие меры? как устранить выявленные недостатки улучшить выполнение процедур ИБ?[5]

Метрики дают нам количественное представление о том в каком состоянии находится СУИБ, с помощью чего мы можем сократить наши затраты на ИБ, на что нам стоит обратить особое внимание, и насколько снизились риски.

Оценку эффективности СУИБ можно рассматривать как системный процесс получения и оценки объективных данных о текущем состоянии систем, помогает установить уровень соответствия СУИБ выставленным критериям.

Более точную оценку эффективности СУИБ можно провести только при помощи ряда методов.

Система сбалансированных показателей оценивает зрелость и компетентность повседневной деятельности управления рисками и ИБ. Данная система показывает эффективность ИБ и управления рисками, отображает соответствие стандартам безопасности, помогает организации развивать единую систему управления рисками, упрощает руководству зрело оценивать состояние СУИБ.[4]

Так же для комплексной оценки эффективности

СУИБ применяют ключевые рисковые показатели, которые способны показать , где организация подвергается риску или где есть высокая вероятность риска, или риск превышает допустимый уровень. Применение ключевых рисковых показателей дает возможность раннего предупреждения для выявления потенциальных событий, которые могут повредить непрерывности деятельности организации.

Test of Operating Effectiveness и Test Design Effectiveness – это метод оценки и мониторинга СУИБ, основанное на тестировании эффективности внедренных мер безопасности.

Test Design Effectiveness дает возможность понять действительно ли выбранные меры безопасности могут уменьшить риск и насколько они эффективны.

Test of Operating Effectiveness показывает нам действительно ли выбранные меры безопасности внедрены и работают так. Как было задумано.[4]

Основная проблема с которой сталкивается специалист в области информационной безопасности при оценке эффективности СУИБ – это недостаточное количество литературы направленной на решение данной проблемы. Так же важным аспектом для решения данной задачи является наличие законодательной базы в данной отрасли информационной безопасности.

ЗАКЛЮЧЕНИЕ

Оценка эффективности СУИБ является важным аспектом в процессе обеспечения ИБ организации. С помощью применения на практике основных методов оценки эффективности СУИБ специалист в области информационной безопасности может не только предоставлять понимаемый отчет по работе СУИБ на организации для руководства, но так же дает почву для полного анализа системы, при помощи которого специалист может наглядно увидеть насколько эффективны применимые меры по защите информации на предприятии, где и с помощью чего можно сократить расходы на реализацию и правильное функционирование СУИБ, насколько реализованные методы снизили риски и т.д.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Н. Куканова «Оценка эффективности мер обеспечения ИБ» (электронный ресурс)/ способ доступа: URL: www.ptsecurity.ru;
2. А. Костина «Оценка эффективности и метрики ИБ» (электронный ресурс)/ способ доступа: URL: http://www.itsec.ru/articles2/control/ocenka-effektivnosti-i-metriki-ib;
3. В. Сысоев «Оценка эффективности СУИБ» (электронный ресурс)/ способ доступа: URL: auditagency.com.ua ;
4. Д. Стуров «Оценка эффективности системы управления ИБ; Метрики информационной безопасности» (электронный ресурс)/ способ доступа: URL: http://www.gosbook.ru .

УДК 65.012.8:621.3.038.616

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ПРЕПЯТСТВОВАНИЮ НОРМАЛЬНОЙ РАБОТЫ В СИСТЕМЕ ВИДЕОНАБЛЮДЕНИЯ

Чередниченко Оксана Игоревна, Научный руководитель: ас. Начовный И.И.
Государственное ВУЗ «Национальный горный университет», http://bit.nmu.org.ua, kcusha_8a1@ukr.net

В данном докладе рассматривается перечень нескольких из возможных способов выведения видеонаблюдения из строя. Так же, далее представлены основные и эффективные методы противодействия препятствованию нормальной работы в системе видеонаблюдения. Данный доклад актуален в сфере информационной безопасности.

Ключевые слова – информационная безопасность; видеонаблюдение; система видеонаблюдения.

ВСТУПЛЕНИЕ

В настоящее время все больше кампаний и просто физических лиц стараются обеспечить полноценную защиту своим объектам не зависимо от того защищают они информацию конфиденциальную или секретную или просто материальные ценности. С каждым днем вандализм и количество изощренных методов препятствованию нормальной работы в системе видеонаблюдения растет. Но, не смотря ни на что, система видеонаблюдения должна функционировать нормально и вовремя предупреждать владельца о потенциальной угрозе. Далее рассмотрим несколько методов борьбы с возможными препятствованием нормальной работы в системе видеонаблюдения.

МЕТОДИКА И РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Проанализировав различные форумы на темы «Как вывести систему видеонаблюдения из строя», «Нейтрализации камер слежения» и т.д., был выбран следующий перечень некоторых из возможных способов выведения системы видеонаблюдения из строя:

- Расположение рядом с системой видеонаблюдения электроприбора с излучением большой мощности.
- Использование рядом с системой видеонаблюдения генератор помех и белого шума (борьба с беспроводными камерами).
- Нарушение целостности элементов системы видеонаблюдения прямым вмешательством: разрыв кабеля, механические повреждения самой камеры.
- Ухудшение видимости камеры: заклеить объектив, залить краской, и т.д..
- Повышение температуры в помещении (борьба с теплокамерами).

- Засветить матрицу солнечными лучами.
- Подача 220В к видеовыходу.
- Засветить инфракрасный датчик (для камер, которые реагируют на движение).

АНАЛИЗ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Рассмотрим каждый способ отдельно и соответствующее возможное решение.

Расположенный рядом электроприбор с излучением большой мощности может снизить сигнал видеокамеры или вовсе погасить его. Он сбивает точные настройки системы видеонаблюдения, и нарушают процесс синхронизации работы видеокамер всей системы, и ухудшает качество сигнала [1]. Также могут быть использованы против системы видеонаблюдения побочные электромагнитные излучения и наводки. Решением в данном случае – использование системы с двухсторонним протоколом обмена: обязательное подтверждение получения сообщения о срабатывании инфракрасного датчика (квитирование). Если извещатель, передающий контрольные сигналы, не получив квитанцию от приемно-контрольного прибора после передачи тестового сигнала, немедленно задействует один из следующих методов: автоматическая регулировка периода выхода в эфир, автоматическая регулировка мощности излучения, автовыбор резервных каналов.

Нарушение целостности элементов системы видеонаблюдения. В данном методе вариантов препятствованию нормальной работы системы видеонаблюдения очень много: начиная от закрашивания объектива краской, мебельным воском, силикатным клеем, заклеиванием изолентой, жвачкой, кинутым в камеру камень и заканчивая огнестрельным оружием, взрывчаткой и т.д.[2] К сожалению, антивандального кожуха в данном случае будет мало. Для начала необходимо правильно спроектировать систему видеонаблюдения, чтобы каждая камера была в поле зрения другой. Большинство современных видеокамер оснащены функцией «защиты от закрашивания», но эта опция по умолчанию отключена, и большинство специалистов даже не знают, что она есть в самой камере. От повреждения кабеля рекомендуется использовать металлические трубы. Также необходимо настроить систему видеонаблюдения, чтобы система реагировала на пропадание видеосигнала от камеры как на тревогу, т.о. на пост охраны сразу будет послан соответствующий сигнал.

Если на объекте установлены теплокамеры, то необходимо установить чувствительность датчика тепла на предельно высокую температуру ниже температуры тела человека, чтобы при повышении температуры в помещении он подал на приемно-контрольный пункт сигнал тревоги.

Попытки засветить матрицу камеры отраженными солнечными лучами решается путем установки на объекте камер, оснащенных системой автоматической регулировки диафрагмы. При попадании прямых и отраженных солнечных лучей объектив просто закроется. Также рекомендуется настроить включение соседних камер, в случае закрытия объектива.

Подключение к видеовыходу 220v. Видеовход не пострадает, если установлена защита от перенапряжения видеосигнала и камера подключена по сети, а не по коаксиалу. Но если камера подключена уже по коаксиалу, то в случае отключения на мониторе увидят VIDEO LOST. Если к камере идет только один кабель (нет отдельных проводов питания, видеовыхода), то, скорее всего, это сетевая камера с питанием по тому же проводу (PoE). В таком случае при подключении к видеовыходу 220В могут сгореть свитч/роутер и/или инжектор/блок питания PoE. Видеокамерам необходимо питаться от отдельного блока питания, а у регистратора должен быть тоже свой отдельный блок питания [3].

Если произвести фотографирование датчика движения в упор, то можно вывести из строя светочувствительный пироэлектрический детектор, который после такого воздействия может значительно ухудшить свои качества по обнаружению перемещения объектов в зоне его действия. Либо используют инфракрасный прожектор и направляют на датчик. В итоге он слепнет. Естественно, в этот момент датчик сработает, но успокоившись, не будет видеть ничего. И если охранник не проверит работу датчика, то на дальнейшие действия злоумышленника датчик перестанет срабатывать. В данном случае возможно установить радиоволновые датчики. Они работают как радар, излучают СВЧ, и принимают отраженный сигнал. Преимущество в том, что просвечивают насквозь небольшие препятствия (если загородить, например, коробкой). Их ставят, как правило, напротив окон со ставнями (металл не пропускает волны), чтобы они реагировали на взлом окон.

ВЫВОДЫ

Был приведен перечень самых популярных способов выведения системы видеонаблюдения из строя и можно еще много найти способов подбора метода противодействия к каждому из способов. Но самое первое правило при проектировании системы видеонаблюдения – это, чтобы система видеонаблюдения обеспечивала полную видимость камер друг другу и отсутствовали мертвые зоны. Дальше необходимо подобрать правильно камеру, чтобы она, насколько это максимально возможно, удовлетворяла все требования видимости, безопасности и защиты от помех внешней среды, если это камеры наружного видеонаблюдения. Если бюджет на проектирование системы видеонаблюдения выходит больше, чем рассчитывает владелец, необходимо пересчитать, сколько обойдется полученный ущерб и возобновление системы видеонаблюдения, в случае вывода её из строя.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Монтаж видеонаблюдения, обслуживание видеонаблюдения (Электр. ресурс) / Способ доступа: URL: http://www.montajgrad.ru/installation_of_cctv/. – Заглав. с экрана

2. Как вывести из строя камеры видеонаблюдения (Электр. ресурс) / Способ доступа: URL: http://www.bolshoyvopros.ru/questions/589672-kak-vyvesti-iz-stroja-kamery-videonabljudenija.html/. – Заглав. с экрана.

3. Убить камеру видеонаблюдения (Электр. ресурс) / Способ доступа: URL: http://phreaker.us/forum/showthread.php?t=15879/. – Заглав. с экрана.

УДК 004.056

ЗАЩИТА РЕЧЕВОЙ ИНФОРМАЦИИ В ВЫДЕЛЕННЫХ ПОМЕЩЕНИЯХ ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ И ВИБРОАКУСТИЧЕСКОМУ КАНАЛАМ

Линник Ю.Ю., Войцех С.И.

ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, Linnikjj@gmail.com

Проведен анализ акустического и виброакустичексого технических каналов утечки речевой информации в выделенном помещении. Рассмотрены достоинства и недостатки пассивных и активных методов защиты от утечки речевой информации. Сделан вывод о необходимости комплексного подхода к их применению

Ключевые слова: речевая информация, технический канал, методы защиты, комплексный подход

ВСТУПЛЕНИЕ

Защита акустической речевой информации с ограниченным доступом от утечки по техническим каналам является достаточно дорогим и сложным мероприятием, поэтому на практике в учреждениях и фирмах целесообразно иметь специально организованные места с гарантированной защитой акустической информации.

Выделенное помещение – специальное помещение предназначенное для проведения собраний,совещаний,бесед и других мероприятий в ходе которых озвучивается информация с ограниченным доступом с использованием или без использования технических средств обработки речи.

К техническим каналам утечки речевой информации в выделенных помещениях относятся:

- акустический;
- виброакустический;
- акустоэлектрический;
- за счет ВЧ- навязывания;
- оптико-электронный.

Из них особое внимание требуют акустический и виброакустический технические каналы утечки информации.

• **Акустический канал.** В акустических технических каналах утечки информации основной средой распространения акустических сигналов является воздух, а для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

Микрофоны объединяются или соединяются с портативными звукозаписывающими устройствами (диктофонами) или специальными миниатюрными передатчиками.

Перехваченная информация может передаваться по радиоканалу, оптическому каналу (в инфракрасном диапазоне длин волн), по сети переменного тока, соединительным линиям ВТСС, посторонним проводникам (трубам водоснабжения и канализации, металлоконструкциям и т.п.).

• **Виброакустический канал.**

В виброакустических каналах утечки информации средой распространения акустических сигналов являются строительные конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твёрдые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы).

МЕТОДЫ ЗАЩИТЫ

Защита речевой информации от утечки по акустическому и виброакустическому каналам может осуществляться с использованием пассивных и активных методов защиты.

Пассивные методы защиты речевой информации направлены на:

• ослабление акустических (речевых) сигналов на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения техническим средством разведки на фоне естественных шумов;

• исключение (ослабление) прохождения сигналов высокочастотного навязывания во вспомогательные технические средства, имеющие в своем составе электроакустические преобразователи (обладающие микрофонным эффектом);

• выявление излучений акустических закладок и побочных электромагнитных излучений диктофонов в режиме записи;

Активные методы защиты акустической (речевой) информации направлены на:

• создание маскирующих акустических и вибрационных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного акустического сигнала техническим средством разведки;

• электромагнитное и ультразвуковое подавление диктофонов в режиме записи;

• создание прицельных радиопомех акустическим и телефонным радиозакладкам с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;

К достоинствам активных методов защиты

относятся[2]:

- низкая стоимость первичной реализации;
- возможность точной настройки зашумляющих сигналов, снижающих паразитные шумы;
- возможность обеспечения защищенности различных видов помещений.

К недостаткам относятся:

- необходимость включения и выключения системы защиты на период проведения закрытого мероприятия;
- необходимость периодической инструментальной проверки и настройки;
- надежность системы защиты определяется надежностью генератора шума и датчиков зашумления.

Достоинствами пассивных методов защиты являются:

- отсутствие паразитных акустических шумов;
- высокая временная надежность параметров звукопоглощения и вибропоглощения;
- постоянная защищенность помещения в течении определенного времени;
- отсутствие зависимости от энергоснабжения;
- обеспечение комфортности в помещениях (за счет снижения общего уровня шума).

Недостатками пассивных методов защиты являются:

- применение методов защиты в полном объеме возможно только при строительстве или капитальном ремонте защищаемого помещения;
- изменение параметров защищенности помещения, как правило, требует проведения строительных работ.

ВЫВОДЫ

Для повышения уровня защищенности выделенного помещения от утечки информации по техническим каналам необходим комплексный подход, определяющий состав, стоимость и эффективность мероприятий по технической защите информации с учетом достоинств и недостатков активных и пассивных методов защиты.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь! Москва НОУ ШО «Баярд», 2004 - 432с.

2. «Бюро Научно-Технической информации» Каргашин В.Л.Защита от утечки речевой информации из помещений. Практические аспекты реализации./Способ доступа: URL: http://www.bnti.ru/showart.asp?aid=1024&lvl=04.02.03. - Заглавие с экрана.

УДК 004.056

ИССЛЕДОВАНИЕ ВЛИЯНИЯ КОНФИГУРАЦИИ И ПАРАМЕТРОВ ЛИНИЙ ЭЛЕКТРОПИТАНИЯ ОСНОВНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ НА УРОВЕНЬ ЗАТУХАНИЯ ИНФОРМАЦИОННОГО СИГНАЛА

Носков К.В., Буренко И.В.

ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, E-mail: sempai@inbox.ru

Рассмотрена теория длинных линий, доказана возможность применение теории длинной линии при исследовании цепей электропитания, указаны важные параметры и особенности цепей электропитания.

Ключевые слова – Длинная линия, цепь электропитания, техническая защита

ВВЕДЕНИЕ

При создании комплекса технической защиты информации (КТЗИ) важную роль играет защита от утечки информации по электрическому каналу, так как в силу информационных технологий информация хранится, обрабатывается и передаётся в электронном виде. Анализ конфигураций и параметров сетей электропитания на основе теории длинных линий позволяет оценить цепи электропитания с позиции технической защиты информации.

ОСНОВНАЯ ЧАСТЬ

Длинная линия - это линия электропередачи, длина которой превышает длину волны колебаний распространяющихся в ней, а расстояния между проводниками, из которых состоит данная линия, значительно меньше этой длины волны. Такая линия называется линией электропередач с распределёнными параметрами. Длинная линия характеризуется следующими первичными параметрами:

- погонное сопротивление R_x [Ом/м];
- погонная проводимость G_x [1/Ом·м];
- погонная ёмкость C_x [Ф/м];
- погонная индуктивность L_x [Гн/м].

Распространение сигналов в длинных линиях строго соответствуют математическому описанию физической модели распределённой электрической цепи.

Наиболее часто встречающиеся в практике длинные линии:

- Коаксиальный кабель – длинная линия, одним проводником которой является центральная жила, а вторым проводником служит металлическая оплётка, между жилой и оплёткой находится цилиндрический слой диэлектрика;
- Двухпроводная линия (фидер) характеризуется двумя геометрическими размерами – расстоянием между двумя проводниками и диаметром этих проводников;

- Полосовая (полосковая) линия образуется двумя параллельными плоскостями шириной l, расположенными на расстоянии h друг от друга.

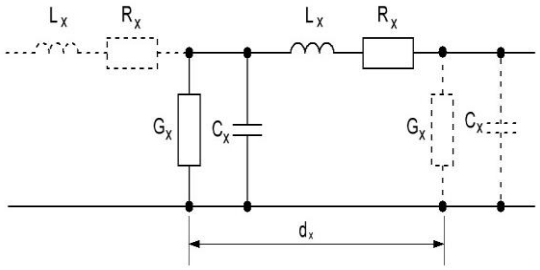

Рисунок 1. Эквивалентная схема бесконечно малого отрезка длинной линии

Теорию длинных линий можно применить для изучения распространения информационных сигналов в сетях электропитания основных технических средств, так как диапазон частот этих сигналов от сотен Гц до нескольких десятков ГГц. Следовательно, для сигнала частотой в 10 МГц длина волны будет равняться согласно формуле (1)

$$\lambda = \frac{c}{f} = \frac{300 \cdot 10^6 \, м/с}{10 \cdot 10^6 \, Гц} = 30 \, м, \qquad (1)$$

где λ – длина волны; c – скорость света; f – частота сигнала.

Таким образом, линия электропередач свыше 100 м для электромагнитной волны с частотой 10 МГц будет длинной линией, или линией с распределёнными параметрами.

Первичные параметры длинных линий зависят от материала проводников, диэлектриков, структуры расположения жил в проводе, в соответствии с формулами (2,3,4).

$$L_x = \frac{\mu_0 l}{\pi}\left(\ln\frac{D}{r} + \frac{\mu_r}{4}\right) \qquad (2)$$

где μ_0 – магнитная постоянная; l – длина линии; D – расстояние между проводниками; r – радиус проводников; μ_r – магнитная проницаемость диэлектрика.

$$C_x = \frac{\pi \varepsilon \varepsilon_0 l}{\ln\frac{D}{r}} \qquad (3)$$

где ε – диэлектрическая проницаемость диэлектрика; ε_0 – электрическая постоянная среды; l – длина линии; D – расстояние между проводниками; r – радиус проводников.

$$R_x = 2 \cdot \frac{\rho l}{S} \qquad (4)$$

где ρ – удельное сопротивление проводника; l – длина линии; S – поперечное сечение проводника.

Некоторые из кабелей, применяющихся в сетях электропитания помещений, приведены ниже:

- кабель ВВГ - круглый или плоский кабель для прокладки внутри помещений с нормальной влажностью. Проводники медные. Количество жил в кабеле - от 1 до 4.
- кабель АВВГ - круглый или плоский кабель для прокладки внутри помещений с нормальной влажностью. Проводники алюминиевые. Количество жил в кабеле - от 1 до 4.
- кабель ПВС - круглый кабель медными проводниками.
- кабель ШВВП - плоский кабель с медными проводниками.

При расчётах длинных линий с учётом параметров передаваемых сигналов, используются вторичные параметры длинных линий: коэффициент затухания α, коэффициент фазы β и волновое сопротивление Z_B . Вторичные параметры длинной линии зависят не только от материала, структуры проводников, материала диэлектрика, но и от частоты электромагнитной волны (5,6,7).

$$\alpha = \frac{1}{\sqrt{2}}\sqrt{R_x G_x - \omega^2 L_x C_x + \sqrt{(R_x^{\,2} + \omega^2 L_x^{\,2})(G_x^{\,2} + \omega^2 C_x^{\,2})}} \qquad (5)$$

где ω – циклическая частота электромагнитной волны.

$$\beta = \frac{1}{\sqrt{2}}\sqrt{\omega^2 L_x C_x - R_x G_x + \sqrt{(R_x^{\,2} + \omega^2 L_x^{\,2})(G_x^{\,2} + \omega^2 C_x^{\,2})}} \qquad (6)$$

$$Z_B = \sqrt{\frac{R_x + \imath\omega L_x}{G_x + \imath\omega C_x}} \qquad (7)$$

Важную роль играют подключенные в сеть электропитания нагрузки. Помимо активного сопротивления, вносится и реактивное сопротивление. Таким образом, при исследовании влиянии параметров линии электропитания основных технических средств на уровень затухания информационного сигнала, необходимо учитывать и конфигурацию линии: какие нагрузки подключены, на каком расстоянии, характер вносимого сопротивления.

ЗАКЛЮЧЕНИЕ

Обоснована возможность применения при исследовании цепей электропитания теории длинных линий. Приведены: описание распространённых видов длинных линий, и кабелей из которых они состоят; расчётные формулы подтверждающие влияние параметров линии электропитания на прохождение информационных сигналов в них.

СПИСОК ЛИТЕРАТУРЫ

1. Стариковская С.М. Физические методы исследования: Учебно-методическое пособие. — М.: МФТИ, 2004. - 156 с.

2. Временные рекомендации по технической защите информации в средствах вычислительной техники, автоматизированных системах и сетях от утечки по каналам побочных электромагнитных излучений и наводок. (ТР ЭВТ-95)

УДК 004.896

ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ АС УПРАВЛЕНИЯ ВУЗОМ

Герасименко А.В., Научный руководитель: д.т.н., проф. Бабенко Т.В.
Государственный ВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, Anika_24@i.ua

В работе рассмотрены вопросы применения интеллектуальных систем информационной безопасности для повышения защищенности автоматизированной системы (АС) управления ВУЗом. Актуальность обеспечения информационнои безопасности АС управления ВУЗом обусловлена высокими темпами развития, усложнением инфраструктуры и расширением функциональных возможностеи АС. Перспективным методом разработки систем информационнои безопасности является использование аналогии механизмов защиты информационных процессов биосистем в искусственных системах.

Ключевые слова – интеллектуальные системы информационной безопасности; адаптивные системы; автоматизированная система управления ВУЗом.

ВВЕДЕНИЕ

Автоматизированная система управления высшым учебным заведением как интранет-система подвержена высокому риску нарушения информационной безопасности. Традиционно для обеспечення защиты компьютерных систем в сфере образования используются разрозненные средства информационной безопасности, такие как антивируси, системы обнаружения вторжений, межсетевые экраны и т.д. В то же время практика показывает, что для эффективного предотвращения внешних и внутренних информационных угроз этого недостаточно.

Современные научные достижения в таких областях информатики, как математическое моделирование состояния внешнего мира, искусственныи интеллект, теория принятия решении, обработка изображении, сигналов и сцен, распознавание образов, оптимальное управление, позволяют говорить о реальнои возможности перехода к новому поколению средств информационнои защиты – интеллектуальным системам информационнои безопасности.

ЗАДАЧИ ИНФОРМАЦИОННОИ БЕЗОПАСНОСТИ, РЕШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ МЕТОДОВ И СРЕДСТВ

Для обеспечения защиты и оперативного реагирования на события информационной безопасности требуется построение единой системы защиты информации (СЗИ), обладающей адаптивными своствами. Это позволит формировать и дополнять комплекс механизмов защиты в соответствии с условиями функционирования системы, производить оценку защищенности, отслеживать наиболее задействованные механизмы защиты и в конечном итоге снизить затраты на осуществление защиты информации при необходимом и достаточном уровне информационной безопасности.

Задачи в сфере информационной безопасности, требующие использования методов и средств искусственного интеллекта:

1. Обнаружение вторжении и атак на автоматизированные информационные системы.
2. Организация соответствующего информационного реагирования и противодеиствия.
3. Проведение периодического активного контроля имеющихся средств защиты.
4. Организация автоматизированного аудита событии безопасности.
5. Идентификация и аутентификация пользователеи;
6. Разработка мультиагентных систем.
7. Разработка систем обнаружения знании в базах данных.

На сегодняшний день существует несколько теоретико-практических подходов для решения вышеперечисленных задач:

- Нейронные сети.
- М-сети.
- Системы нечеткой логики.
- Экспертные системи.
- Эволюционные и генетические технологии.
- Мультиагентные технологии.
- Имунные алгоритмы.
- Конечные автоматы.

СРЕДСТВА ОБЕСПЕЧЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ АДАПТИВНЫМИ СВОЙСТВАМИ

Биосистемная аналогия в структуре защиты информационных систем базируется на иерархии СЗИ, встроенных механизмах иммуннои защиты и накопления опыта. Известные СЗИ, как правило, ограничиваются реализациеи функции нижнего уровня системы защиты и антивируснои направленностью средств иммуннои защиты. Для создания комплекснои адаптивнои защиты автоматизированных систем на основе биоаналогии необходимо решать не отдельных задачи защиты информации с помощью нейронных сетей, систем нечеткои логики, экспертных систем, а разработки единого подхода применения интеллектуальных

средств. Проектирование следует осуществлять как единыи процесс построения адаптивнои системы с внутренне присущими функциями защиты информации [1].

Наилучшим сочетанием своиств для достижения поставленнои цели обладают нечеткие нейронных сетей, которые сочетают достоинства нейронных сетей и нечеткои логики, опирающеися на опыт экспертов информационнои безопасности. Механизм нечеткого логического вывода позволяет использовать опыт экспертов, овеществленныи в виде системы нечетких предикатных правил, для предварительного обучения нечеткои нейронной сети. Последующее обучение нейронной сети на поле известных угроз предоставляет возможность анализа процесса логического вывода для коррекции существующеи или синтеза новои системы нечетких предикатных правил СЗИ.

Свойства нечетких нейронных сетей, необходимые для адаптивных СЗИ:

1. Функциональная устоичивость и защищенность элементнои базы.
2. Возможность классификации угроз.
3. Описание соответствия «угрозы – механизмы защиты» в виде системы нечетких предикатных правил.
4. Адаптивность неиро-нечетких СЗИ (системы нечетких правил).
5. «Прозрачность» для анализа структуры связеи неиро-нечетких СЗИ и системы нечетких правил.
6. Распределенныи параллелизм вычислении.

Неиросетевые СЗИ согласно принципу биосистемнои аналогии следует представлять в виде описания структурированных информационных полеи иммунного и рецептороного уровнеи защиты. В качестве языковых средств для описания неиросетевых СЗИ целесообразно использовать язык пакетных неиросетевых программ. В этом случае НС представляется в виде совокупности взаимосвязанных командных пакетов, которая помещается в командных пулах. При описании НС пакетными неиросетевыми программами возможна различная степень детализации: командныи пакет может соответствовать однои из функции неиросетевого логического базиса, функции формального неирона, слоя из формальных неиронов или неироннои сети в целом.

ВЫВОД

Разработка модели адаптивной СЗИ на основе интеллектуальных механизмов нейронных сетей, нечеткой логики, генетически алгоритмов является актуальной научно-техническои задачей, имеющеи существенное значение для обеспечения безопасности АС, подверженных высокому темпу развития и расширения.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Осовецкии Л. Г., Нестерук Г.Ф., Куприянов М.С., Нестерук Ф. Г. Иммунология сложных вычислительных систем // Труды 8-го междунар. НПС "Защита и безопасность вычислительных технологий ". - СПб, 2002. С. 18 - 25.
2. Нестерук Г. Ф., Куприянов М. С., Нестерук Ф. Г. О разработке языковых средств для программирования неиросетевых структур // Сб. докл. V междунар. конф. SCM’2002. - СПб, 2002, Т.2.С. 52-55.
3. Ивахненко А.Г., Савченко Е.А., Ивахненко Г.А., Гергеи Т., Надирадзе А.Б., Тоценко В.Г. Неирокомпьютеры в информационных и экспертных системах // Неирокомпьютеры: разработка и применение. 2003, No 2.
4. Осовецкии Л. Г. Научно-технические предпосылки роста роли защиты информации в современных информационных технологиях // Изв. вузов. Прибо-ростроение. 2003. Т.46, No 7. С.5-18.

УДК 004.056.5

АНАЛИЗ УРОВНЯ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ АВТОМОБИЛЯМИ И РЕКОМЕНДАЦИИ ПО ЕГО ПОВЫШЕНИЮ

Герасименко С.В., Науковий керівник: д.т.н., проф. Бабенко Т.В.
Государственный ВУЗ «Национальный горный университет», http://bit.nmu.org.ua/, shefun@bk.ru

В работе показаны основные моменты, связанные с проблемами информационной безопасностью, при эксплуатации автоматизированных систем управления легковым автомобилем. Актуальность обеспечения высокого уровня защищенности АСУ легковым автомобилем обусловлена увеличивающимся спросом на такие системы и повышением уровня осведомленности и обеспеченности злоумышленников.

Ключевые слова – автоматизированная система управления автомобилем; использование GSM систем в охранных системах.

ВВЕДЕНИЕ

Последнее время наблюдается всплеск роста популярности интеллектуальной техники начиная от «умных» холодильников и до «умных» автомобилей. Почти вся «умная» техника имеет доступ в интернет или может управляться посредством GSM каналов.

По этому если постоянно не совершенствовать средства и методы защиты «умной» техники то у злоумышленников может появиться возможность

воздействовать на нее с целью навредить пользователю или обманув систему защиты обворовать пользователя. Современные «умные» автомобили нуждаются в особой защите так как стоят довольно дорого и часто оставляются в неохраняемых местах (на улицах, неохраняемых парковках) а также могут подвергнуть опасности жизнь пользователя если злоумышленник сможет получить НСД к АСУ автомобиля.

СТРУКТУРА И ПРИНЦИП РАБОТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ АВТОМОБИЛЯМИ

Система управления легковым автомобилем представляет собой программно-аппаратный комплекс, который позволяет:

- Предпринять меры по защите автомобиля при попытке взлома/угона.
- Оповещать пользователя при попытке взлома/угона.
- Удаленно управлять автомобилем.

В соответствии с функциями, АСУ можно логически разбить на несколько логических подсистем:

Центральный модуль - выполняет команды пользователя и реагирует на воздействие окружающей среды (на основании показаний датчиков), принимая меры по защите автомобиля.

Система связи с пользователем - представлена на рис. 1 и может взаимодействовать с пользователем посредством:

Речи / SMS команд - представляет собой канал двухсторонней связи, на рисунке показан пунктирными линиям.

Сети интернет - получив доступ в интернет (используется GPRS канал), автомобиль связывается с сервером и постоянно поддерживает соединение, отправляя на сервер данные о своем состоянии и принимая от него команды. Пользователь в свою очередь тоже связывается с сервером (используя приложение на телефоне) и может наблюдать за состоянием автомобиля, получать уведомления в случае попытки взлома/угона а также отправлять команды управления

Связь с сервером является приоритетной и используется при условиях:

Если автомобилю разрешено использовать GPRS канал (по умолчанию разрешено)

Если достаточно денег на счету

Переключение на режим связи через речь / SMS активизируется при условиях:

Инициатором связи стал пользователь (позвонили или отправил SMS)

Зафиксирована попытка взлома / угона и пользователь не подключен к серверу (приложение на телефоне не запущено или нет доступа в интернет)

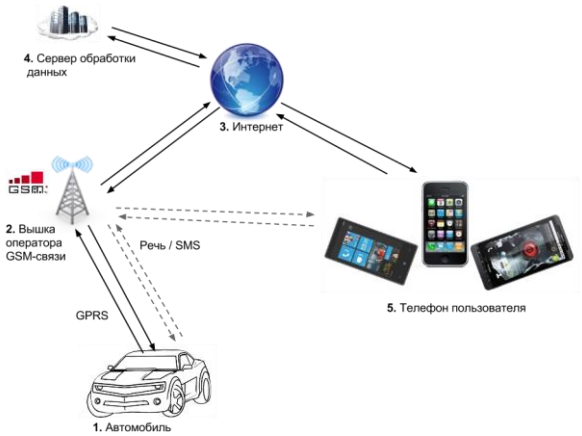

Рисунок 1. Схема каналов коммуникации между пользователем и автомобилем

АНАЛИЗ СУЩЕСТВУЮЩИХ СРЕДСТВ ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ АВТОМОБИЛЯМИ

Исходя из схемы связи автомобиля и с пользователем можно выделить несколько схем воздействия на систему:

Глушение радиоканала (GSM).

- Атака на сервер.
- Подслушивание/подмена трафика в каналах пользователь-сервер, автомобиль-сервер, GSM канала.

1) Воздействие на АС, используя особенности GSM связи.

Как видно из рис.1 связь автомобиля с пользователем происходит по одному из двух возможных каналов GPRS или Голос / SMS, но автомобиль всегда вынужден использовать GSM.

Так как автомобиль всегда вынужден использовать GSM канал, вне зависимости от выбранного способа передачи данных, то если злоумышленник заглушит GSM сигнал - пользователь не получит уведомления и не сможет должным образом отреагировать.

Для устранения это применяются несколько подходов, в зависимости от того какой тип передачи данных выбран.

В случае с GPRS решение этой проблемы ложиться на сервер, так как при этом способе передачи данных соединение с сервером постоянно открыто, а следовательно при разрыве соединения сервер может узнать что сигнал был заглушен и сообщить об этом пользователю.

В случае с Голос / SMS применяется отдельное устройство, которое находится у пользователя и периодически пытается дозвониться до автомобиля и если ему это не удается то оно уведомляет пользователя о потере сигнала.

Также автомобиль может определить факт глушения сигнала и предпринять меры по защите авто (например закрытие замков + сирена что бы отпугнуть злоумышленника).

2) Воздействие на АС через сервер.

Поскольку сервер является связующим звеном между пользователем и автомобилем, то обезвредив сервер (вызвав отказ в обслуживании).

На случай невозможности подключения к серверу автомобиль будет уведомлять пользователя о попытках взлома / угона по каналу Голос / SMS.

3) Воздействие на АС через каналы связи (сниффинг, спуфинг).

Здесь можно выделить 2 возможных точки воздействия:

- GSM канал связи (автомобиль - базовая станция (GPRS),автомобиль - базовая станция (Голос/SMS), пользователь - базовая станция (Голос/SMS).
- Сеть, через которую пользователь получает доступ в интернет.

GSM канал:

Для управления автомобилем посредством Голоса/SMS необходимо знать номер sim карты, установленной в автомобиле и PIN код.

Для получения этих данных злоумышленник может воспользоваться репитером, который регистрируется в системе оператора и выдает себя за базовую станцию, что заставляет абонентов сети в радиусе нескольких десятков метров подкючиться к репитеру. Поскольку служебные данные в GSM передаются в незашифрованном виде то зафиксировать звонок или SMS и злоумышленник получит номер sim карты автомобиля. Для получения PIN кода нужно перехватить SMS / Голос сообщение, в котором будет указываться PIN и расшифровать сообщение, используя утилиты подобные «KRAKEN»

Для защиты используется фильтрация команд по номеру абонента. Номер пользователя заносится во внутреннюю базу автомобиля и если команда поступает с другого номера то она просто игнорируется.

Также возможет вариант перехвата и дешифровки GPRS трафика [1].

Для борьбы используется дополнительное шифрование по алгоритму AES-128.

Локальная сеть пользователя:

Для анализа трафика нужно получить к сети пользователя (обычно телефон подключен по Wi-Fi) и воспользоваться анализатором трафика. В следствии чего злоумышленник может получить PIN код пользователя либо подменить трафик.

Для защиты используется защищенное соединение SSL + дополнительное шифрование по протоколу AES-128.

ВЫВОД

Рассмотренная АСУ легковым автомобилем обладает каскадной системой защиты что в значительно мере усложняет атаку на АСУ. Тем не мнение можно выделить несколько ключевых звеньев (GSM канал связи автомобиля и сервер), воздействовав на которые одновременно злоумышленник сможет оставить пользователя в неведении и осуществить взлом/угон автомобиля. Следовательно для повышения общего уровня безопасности АСУ нужно повысить безопасность самых слабых звеньев. Поскольку нет возможности ничего предпринять против глушения GSM сигнала то стоит повысить зашищенность сервера, применив сетевые экраны и интеллектуальные средства выявления атак.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Система перехвата и дешифровки GPRS (Электр. ресурс) / Способ доступа URL: http://itbuben.org/blog/1474.html.

УДК 628.1:681.5

АНАЛІЗ СУЧАСНОГО СТАНУ СИСТЕМ ВОДОПОСТАЧАННЯ УКРАЇНИ

Дашко Д.О., Науковий керівник: д.т.н., проф. Бабенко Т.В.
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, dashkodo@gmail.com

Несприятливе становище з водопостачанням населення сьогодні розглядається багатьма країнами як загроза національній безпеці у зв'язку з погіршенням з цієї причини здоров'я людей. Тому проблеми підвищення стійкості та надійності функціонування систем водопостачання, як критичних елементів інфраструктури держави, стають в даний час актуальними як ніколи.

Ключовіе слова – системи водопостачання; національна безпека; аналіз стану систем водопостачання.

ВСТУП

Надійність і безпека систем водопостачання та водовідведення є невід'ємним елементом національної безпеки країни. Майже 100% населення в містах користується системами централізованого водопостачання. Хвороби інфекційної або неінфекційної природи з легкістю проникнуть в будь-яке житло у разі ненадійності мереж та відсутності систем аналізу стану води. З іншого боку порушення водопостачання також є реальною загрозою. Разом с тим існуючий стан систем водопостачання на даний момент характеризується, як кризовий.

АНАЛІЗ СУЧАСНОГО СТАНУ СИСТЕМ ВОДОПОСТАЧАННЯ

Водопровідні мережі й водоводи є спорудами у складі систем подачі й розподілу води сучасних населених пунктів і вміщають елементи з різним конструктивним устроєм, технічним ресурсом та мають складну топологію. Такі трубопровідні системи повинні задовольняти вимогам надійного забезпечення всіх споживачів розрахунковими витратами води з необхідним напором при найменших витратах на будівництво й експлуатацію

не тільки самих трубопроводів, що входять до їх складу, але й гідравлічно пов'язаних із ними водопровідних споруд. Проблеми забезпечення надійної й ефективної роботи трубопровідних систем пов`язані з тим, що вони працюють у надзвичайно складних умовах експлуатації, під впливом дії на них різноманітних факторів конструктивного, об`єктивного і суб`єктивного характеру. При цьому суттєво змінюються характеристики надійності й економічності всієї системи водопостачання.

Під системою водопостачання мається на увазі комплекс взаємопов'язаних споруд, призначених для водозабезпечення будь-якого об'єкта або групи об'єктів. Система водопостачання, що забезпечує водою окремі райони або групи населених пунктів, або групи промислових об'єктів, називається районної чи груповою системою водопостачання.

Централізована система водопостачання населеного пункту або промислового підприємства повинна забезпечувати прийом води з джерела, її кондиціонування (якщо це необхідно), транспортування і подачу до всіх споживачів під необхідним тиском. З цією метою в систему водопостачання повинні бути включені: водоприймальні споруди, призначені для отримання води з природних джерел; насосні станції , що створюють напір для передачі води на очисні споруди, в акумулюючи ємкості або споживачам; споруди для обробки води резервуари і водонапірні башти, які є запасними і регулюючими ємкостями; водоводи і водорозподільні мережі , призначені для передачі води до місць її розподілу і споживання. Послідовність розташування окремих споруд системи водопостачання та їх складу можуть бути різними залежно від призначення, місцевих природних умов, вимог водоспоживачів або виходячи з економічних міркувань.[1]

Довжина мереж водопостачання в цілому по Україні з 1990 року зросла на 37-39%, а довжина аварійних мереж — в 6 разів. В 2008 році загальна довжина водогінних мереж становила 182 626,3 км, з них 36,4% або 66 462,5 км потребують негайної заміни. Зношення устаткування в системах централізованого водопостачання й водовідведення становить 63%. У середньому по Україні рівень втрат води в мережах централізованого водопостачання становить – 40,4%, з великим розкидом по регіонах – від 16% до 82%. Незадовільний технічний стан «побутових» мереж призводить до значних втрат питної води в мережах – до 16 млн. куб. м на добу. Відсоток охоплення послугами водовідведення в цілому по Україні становить 66,7%, або менше ніж 50% для середніх міст і понад 75% для великих. У містах, де чисельність населення перевищує 100 тисяч людей, приблизно 80% зібраних стічних вод зазнають механіко-біологічному очищенню. У малих містах очищається близько 45% від загального обсягу зібраних стічних вод. Загальна довжина мереж водовідведення в 2008 році в цілому по країні становила 50 756,5 км, з них вимагало негайної заміни - 17 269,2 км, або 34%. У ЖКГ експлуатується 25% основних фондів України, зайнято 5% працездатного населення. При цьому в аварійному стані перебуває 30% водопровідних і 27% каналізаційних мереж. На ліквідацію аварій витрачається в 2-3 рази більше засобів, ніж на профілактику або заміну труб у мережах.[2]

АНАЛІЗ СТАНУ АВТОМАТИЗАЦІЇ З ОГЛЯДУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

АСУ ТП водопостачання являють собою вищий етап автоматизації водопровідних споруд і покликані забезпечувати оптимальне ведення технологічних процесів водопостачання. У технологічному процесі водопостачання можна виділити два подпроцесса - підйом і обробку води, подачу і розподіл води. Відповідно до цього під АСУ ТП водопостачання слід розуміти комплекс систем, що складається з:

- АСУ ТП підйому і обробки води (АСУ ТП ПОВ), що здійснює управління насосними станціями 1-го підйому і водоочисними спорудами;
- АСУ ТП подачі і розподілу води (АСУ ТП ПРВ), що охоплює резервуари чистої води, насосні станції 2-го і наступних підйомів, водопровідні мережі.

Основними функціями АСУ ТП є:

- Централізований контроль та облік стану об'єктів водопостачання та діагностика техногологічного процессу.
- Визначення раціонального режиму роботи.
- Визначення режиму роботи у разі надзвичайних ситуацій у системах водопостачання (аварія, відхилення показників технологічного процесу від норми тощо).

Автоматичне управління кожної з насосних станцій та установок, які входять в систему подачі і розподілу води, слід передбачати з урахуванням її взаємодії з іншими насосними станціями системи (в тому числі загальносистемними і локальними станціями підкачки), а також з регулюючими ємкостями та регулюючими пристроями на водоводах і мережі. При цьому слід контролювати зміну подачі води нерегулюючими насосами (в результаті їх саморегулювання) з тим, щоб вони не виходили за межі допустимого діапазону кожного з насосів. В необхідних випадках слід обмежити неприпустиме збільшення подачі води дроселюванням, а неприпустиме її зниження - рециркуляцією. Автоматичне управління роботою систем, як єдиного цілого, має забезпечити подачу необхідної добової витрати води при мінімальних сумарних витратах потужності всіма спільно працюючими насосами, забезпечення вільних напорів в мережі не нижче необхідних і зниження до можливого мінімуму надлишкових вільних напорів, що викликає збільшення витрат води внаслідок витоків та нераціонального витрачання.[3]

З точки зору імплементації АСУ ТП підйому і обробки води та АСУ ТП подачі і розподілу води є автоматизованими системами третього класу, що повинні забезпечувати підвищенні вимоги до цілісності та доступності данних, що входять до інформаційних потоків технологічних процесів.

ВИСНОВКИ

1. Водопровідна мережа і водоводи (трубопровідна система) є системою масового обслуговування, до якої ставлять вимоги надійності та економічної ефективності. Сьогодні діючі трубопровідні системи водопостачання не відповідають цим вимогам у багатьох містах і населених пунктах України;

2. Надійність і безпека систем водопостачання та водовідведення є невід'ємним елементом національної безпеки країни. Майже усе міське населення в містах користується системами централізованого водопостачання, тому порушення водопостачання взагалі чи порушення санітарних норм води у системах водопостачання регіону є загрозою національного масштабу.

3. Марно втрачається майже 30% води та 25% електроенергії на її транспортування через незадовільний стан обладнання трубопроводів, зменшення їхньої пропускної спроможності, через значні витоки води й нераціональне використання води споживачами.

4. Основними причинами незадовільного стану трубопровідних систем водопроводу є значний вік трубопроводів, складні умови їх роботи, неякісне виконання будівельно-монтажних, аварійно-відновлювальних робіт та поточних і капітальних ремонтів, наявність у складі трубопровідних систем елементів різної конструктивної надійності (особливо стикових з'єднань, зварних швів при поєднанні окремих елементів).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Соков М.А. Водопроводные сети и сооружения. М.: Стройздат, 2003. — 129 с.
2. Обзор участия частного сектора в водоснабжении и водоотведении стран ВЕКЦА. Институт экономики города. 2010г.
3. Водопостачання. Зовнішні мережі та споруди. Основні положення проектування: ДБН В.2.5-74:2013 / Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України. – Київ, 2013. –287 с

УДК 65.012.8

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТОРГОВЫХ ПРЕДПРИЯТИЙ

Васютинский О.И., Научный руководитель: ст. викл. Галушко С.А.
Государственный ВУЗ "Национальный горный университет", http://bit.nmu.org.ua/

В данной статье рассмотрены способы обеспечения информационной безопасности торгового предприятия с помощью технических и программных средств. Описываются основные направления, по которым должно проводиться обеспечение информационной безопасности на торговых предприятиях.

Ключевые слова: информационная безопасность, защита, информационное пространство, торговое предприятие.

На крупных торговых предприятиях существуют специальные службы в задачи которых входит обеспечение ИБ, выявление, локализация и устранение угроз ИБ предприятия.

В тоже время ИБ торговых предприятий с не очень большим количеством рабочих мест для специалистов уделяется не слишком много внимания. Обычно такие предприятия имеют не слишком большой бюджет, позволяющий приобрести только необходимое оборудование, ПО и содержать одного системного администратора.

В первую очередь строится модель угроз ИБ предприятия.

Только понимание всего спектра угроз позволит построить эффективную систему защиты.

Формирование политики в области рисков подразумевает определение принципов управления рисками для всей компании в целом. Эти принципы базируются на целях компании, ее стратегии, а также на требованиях, предъявляемых законом и стандартами в области информационной безопасности. Одним и ключевых факторов успешности системы управления информационной безопасностью торгового предприятия - это построение ее на базе международных стандартов ISO/IEC 17799:2005 и ISO/IEC 27001:2005

По отношению к торговому предприятию угрозы делятся на внутренние и внешние. Таким образом хакерская атака на компьютеры будет рассматриваться как внешняя угроза, а занесение вируса в сеть сотрудниками - как внутренняя.

По цели можно выделить угрозы, направленные на получение данных, уничтожение данных, изменение или внесение данных, нарушение работы ПО, контроль над работой ПО и прочие.

Скажем, одной из наиболее частых хакерских атак на компьютеры предприятий является получение закрытых сведений для дальнейшего их незаконного использования (пароли к интернет-банкам, учётным записям электронной почты и т.д.). Такую угрозу можно классифицировать как внешнюю преднамеренную угрозу, направленную на получение данных.

Для построения сбалансированной системы информационной безопасности торгового предприятия предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для организации на основе заданного критерия. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

ВЫБОР КОНТРМЕР

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих

риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут являться рекомендации по проведению регулярных проверок эффективности системы защиты.

УПРАВЛЕНИЕ РИСКАМИ

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

ОЦЕНКА ДОСТИГАЕМОЙ ЗАЩИЩЕННОСТИ

В завершение работ, можно будет определить меру гарантии безопасности информационной среды Заказчика, основанную на оценке, с которой можно доверять информационной среде объекта.

Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности. Адекватность оценки основана на:

- вовлечении в процесс оценки большего числа элементов информационной среды объекта Заказчика;
- глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения;
- строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

Ключевые показатели эффективности могут быть измерены при помощи, например, ARIS Process Performance Manager, а затем интегрированы в систему управления рисками. Также на этой стадии выполняется мониторинг заранее установленных мероприятий, нацеленных на уменьшение объема убытка или частоты появления рисков. Результаты данного процесса могут использоваться в целях аудита для подготовки компании к сертификации по стандарту ISO/IEC 27001:2005.

Следует также понимать, что нельзя защититься от всех мыслимых и немыслимых угроз И.Б хотя бы потому, что невозможно предусмотреть действия злоумышленников, не говоря уж обо всех ошибках пользователей. Однако существует ряд общих методов защиты, которые позволят сильно понизить вероятность реализации широкого спектра угроз и обезопасить торговое предприятие от различного рода атак и ошибок пользователей. Далее мы подробнее рассмотрим наиболее эффективные из них.

Следует по возможности отказаться от применения беспроводных сетей на предприятии, поскольку имеющиеся в продаже недорогие точки доступа не обеспечивают нужного уровня безопасности, а применение криптостойких алгоритмов шифрования при передаче данных подпадает под государственное регулирование, и для этого необходимо получать соответствующие разрешения и лицензии.

Также необходимо строго разграничить доступ пользователей к определённым данным, чтобы ни один пользователь, за исключением доверенных лиц, не имел полного доступа ко всей информации разом. Скажем, в СУБД это делается путем наложения ограничений на выборку определённых полей и строк из БД.

Одним из неплохих вариантов организации хранения данных будет установка системы управления версиями документов и файлов. Существуют очень хорошие бесплатные системы, вроде CVS или Subversion, которые позволяют восстанавливать файл определённой версии или вести мониторинг изменений, то есть пользователь не перезаписывает файл, а добавляет новую версию файла, не удаляет файл, а добавляет новую версию каталога и т.д.

Не стоит забывать и про обучение пользователей: если возможно, пусть системный администратор еженедельно проводит 30-минутный семинар для пользователей предприятия, на котором ненавязчиво рассказывает об основных правилах ИБ и возможных угрозах, с которыми могут столкнуться рядовые пользователи. Несколько живых примеров из повседневной практики помогут лучше усвоить урок и получить удовольствие от этого семинара, а руководство будет иметь дополнительную возможность контролировать ИБ организации.

ИСПОЛЬЗОВАНИЕ МЕЖСЕТЕВОГО ЭКРАНА

Одним из наиболее эффективных методов защиты сети предприятия от внешних угроз является использование межсетевого экрана – программного или аппаратного маршрутизатора, совмещённого с firewall (особой системой, осуществляющей фильтрацию пакетов данных).

ЗАЩИТА ЭЛЕКТРОННОЙ ПОЧТЫ

Следует уделить особое внимание защите электронной почты, так как вредоносные программы часто рассылают сами себя ничего не подозревающим пользователям.

Обязательно следует поставить антивирус на корпоративный сервер электронной почты. При выборе антивирусного пакета нужно руководствоваться следующими принципами:

- антивирус должен уметь переименовывать исполняемые файлы (в которых не найдено вируса), делая невозможным их автоматический запуск пользователем, например, файл с именем **«picture.jpg.exe»** будет переименован в файл с именем **«picture.jpg.exe.tmp»**, что сделает невозможным запуск его пользователем без сохранения на диск и переименования;
- антивирус должен уметь проверять архивированные файлы;
- антивирус должен уметь проверять HTML-код

на предмет вредоносных сценариев и приложений Java, а также вредоносных ActiveX-компонентов.

АНТИВИРУСНАЯ ЗАЩИТА

На компьютеры пользователей следует установить антивирусное ПО, которое будет непрерывно проверять все загружаемые файлы. Это позволит избежать заражения компьютеров пользователей известными вирусами. Хорошим выбором в этом случае будет бесплатная система, например AVG. Однако обновляется она исключительно с сайта компании-разработчика, а если 50 компьютеров одновременно будут загружать обновления с сайта, то сеть предприятия может оказаться перегруженной. Поэтому требуется принять определённый способ обновления антивирусного ПО: либо это будет последовательное обновление с каждого компьютера (настраивается временем запуска обновления), либо обновление с корпоративного сервера (что требует определённой ежедневной работы системного администратора).

Не стоит забывать и про обучение пользователей: если возможно, пусть системный администратор еженедельно проводит 30-минутный семинар для пользователей предприятия, на котором ненавязчиво рассказывает об основных правилах ИБ и возможных угрозах, с которыми могут столкнуться рядовые пользователи. Несколько живых примеров из повседневной практики помогут лучше усвоить урок и получить удовольствие от этого семинара, а руководство будет иметь дополнительную возможность контролировать ИБ организации.

СПИСОК ЛИТЕРАТУРЫ

1. Крошилин С.В., Медведева Е.И. Информационные технологии и системы в экономике. М.: ИПКИР,2008.-485с.
2. Крошилин С.В. Возможные угрозы безопасности экономических информационных систем и методы их устранения: Материалы межвузовской научной конференции профессорско-преподавательского состава. Коломна: КГПИ, 2006. - 240с.
3. Журнал «Технологии разведки для бизнеса» (Электрон. ресурс) / Способ доступа ULR:– Загол. с экрана.

УДК 65.012.8

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В УПРАВЛІННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Маліков Євгеній Вадимович, Мартиненко Андрій Анатолійович
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, petrykivka@mail.ru

Розглядається система підтримки прийняття рішень (СППР) і можливість його застосування в процесі управління інформаційної безпеки. Наводиться практична ефективність використання системи. Робляться висновки, щодо ефективності СППР.

Ключові слова: прийняття рішень, інформаційна безпека, СППР.

ВСТУП

“Хто володіє інформацією, той володіє світом” і з словами Вінстона Черчіля важко сперечатися, тим паче під час інформаційної ери. Сміливо можна стверджувати, будь-яка інформація має свою ціну будь-то державна таємниця, конфіденційна інформація або публічно розголошені данні. Таким чином постає питання у організації інформаційної безпеки та раціональному управлінні. Забезпечення цілісності, доступності, та конфіденційності інформації являється головним завданням інформаційної безпеки. Цього можна досягти лише комплексно та системно, використовуючи організаційні та технічні заходи. Важливим моментом є повнота визначення моделі порушника та моделі загроз, це дасть змогу ліпше зрозуміти що захищати та від кого. Врахування законодавчих баз, національних та міжнародних, є іще одним обов’язковим фактом в управлінні інформаційної безпеки. Таким чином стає зрозумілим що суб’єкту інформаційних відносин треба вирішити безліч питань, при чому ці питання мають бути безкінечними, з міркувань того, що процес управління інформаційної безпеки безперервний, адже з часом жодна модель не зможе врахувати виникнення принципово нових загроз відмінних за природою та алгоритмом реалізації. Для поліпшення процесу вирішення питань керівником існує багато способів, один із них використання системи підтримки прийняття рішень. [1-4]

ОСОБЛИВОСТІ ТА ЕТАПИ СППР

СППР — це інтерактивна комп'ютерна система, яка призначена для підтримки різних видів діяльності при прийнятті рішень із слабо-структурованих або неструктурованих проблем. Головна її мета - підняття ефективності. Вирізняють такі основні методи: інформаційний пошук, інтелектуальний аналіз даних, пошук знань в базах даних, судження на основі прецедентів, імітаційне моделювання, еволюційне вираховування, генетичні алгоритми, нейронні мережі, ситуаційний аналіз, когнітивне моделювання. Застосування СППР забезпечує виконання ґрунтовного та об’єктивного аналізу предметної області при прийнятті рішень в складних умовах. Залежно від даних, з якими ці системи працюють, їх можна умовно поділити на оперативні та стратегічні рішення. Оперативні призначені для негайного реагування на зміни поточної ситуації у керуванні процесами компанії. Стратегічні орієнтовані на аналіз значних обсягів різнорідної інформації, котра збирається із різних джерел. Величезною перевагою даної системи це можливість обробки та з важення великої кількості інформації, при чому у короткі терміни, це дає відчутну перевагу перед недоліками людського фактору. Характерно, що чим більше даних

оброблює система тим більше аргументований та глибше проаналізований буде результат. Розробники системи повинні ретельно вивчити предметну область в, якій вона функціонуватиме та в процесі побудови орієнтуватися на задачі, які перед ними стоять. Для раціональнішого використання результатів СППР слід провести класифікацію видів рішень наведену у табл.1.

Класифікація видів рішень		
№	**Ознака**	**Вид рішення**
1	Ступінь структуризації проблеми	Гарно структуроване Погано структуроване Не структуроване
2	Кількість етапів реалізації рішення	Статичне (один етап) Динамічне
3	Рівень інформованості про стан проблеми	Умови визначеності Умови ризику Умови невизначеності
4	Кількість ОПР	Одна особа Багато осіб
5	Зміст рішення	Стратегічне Тактичне

ПРОЦЕС ПРИЙНЯТТЯ РІШЕНЬ

Безпосередньо процес прийняття рішення складається з трьох основних етапів.

1. Етап постановки задачі. Складається з фаз аналізу та діагностики проблеми і визначення цілей рішення. На цьому етапі відбувається виявлення та опис проблемної ситуації, збір релевантної інформації і даних; визначаються цілі рішення, яке має бути прийняте, що дозволяє задати напрям пошуку рішень і видалити ті, котрі не відповідають цілям.
2. Етап формування рішень. Складається з фаз формулювання обмежень і критеріїв прийняття рішень та визначення альтернатив рішення. На даному етапі відбувається визначення обмежень, що дозволяють відокремити прийнятні варіанти від неприйнятних, та критеріїв, які сприяють вибору кращих з придатних варіантів рішення. Потім здійснюється формування множини допустимих альтернатив, яке полягає у пошуку та розробці альтернативних варіантів рішення.
3. Етап вибору рішення. Складається з фаз оцінки альтернатив та остаточного вибору рішення. На даному заключному етапі відбувається оцінка варіантів з множини допустимих альтернатив за обраними критеріями та подальший остаточний вибір рішення. Цінність альтернативних варіантів звичайно не однакова, але за умов неявної переваги одного варіанту перед іншим можуть виникати певні складності.

Більшість рішень в сучасних складних задачах приймаються людиною одноособово або колегіально в умовах наявності невизначеностей. СППР, очевидно з вище наведених даних, не приймає рішення а дає вихідні аналітично сформовані данні, які спрямовані на полегшення і обґрунтування правильності прийняття рішення. Для управління інформаційною безпекою СППР слід розцінювати не як захід протидії зловмисникам, а як додаткові структуровані програми допомоги для прийняття рішення. Важливо підкреслити, що під час етапу удосконалення в структурі функціонування СУІБ (ISO 27001) керівнику доводиться приймати рішення в обставинах невизначеності та багатогранності питання, а застосування СППР значно полегшить сформувати аналітичне обґрунтування можливих варіантів. Слід врахувати швидкість отримання результатів обробки даних що в свою чергу зменшить час для вжиття заходів, що для ИБ конче важливо. Розглядаючи питання обробки ризиків в ІБ керівник, використовуючи СППР, адаптовану під обробку певних даних , зможе глибше зважити ціну питання. Як відомо, одним із можливих посередників цінної інформації – це людина, адже вона управляє системою та має доступ до даних які треба захистити, тому підбір кадрів має важливе значення для інформаційної цілісності підприємства, а використання СППР може зменшити можливість підбору кадрів , які мають схильність і більшу вірогідність до крадіжки цінних даних. Прикладом є процедура проходження тестування на поліграфі, лише в тому разі якщо майбутній співробітник оперуватиме важливою інформацією. Таку практику можна використати і в різних галузях.

ВИСНОВОК

За результатами аналізу очевидно, що система підтримки прийняття рішень ефективний, стрімко розвиваючийся спосіб раціоналізації керівницької діяльності. Розмаїття методологій даної системи і надалі знаходитиме застосування не тільки в управлінні інформаційною безпекою а й у інших напрямках. Її практична користь та беззаперечна доцільність перетворюватиметься в повсемісне впровадження.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Система підтримки прийняття рішень. – (Електр. ресурс) Спосіб доступу: URL: http://ru.wikipedia.org/wiki/СППР. – Загол. З екрану.
2. М.В. Грайворонський, О.М. Новіков. Безпека інформаційно-комунікаційних систем.
3. Урінцов А.И. Дик В.В. Система підтримки прийняття рішень.
4. Бідюк П.І., Гожий О.П., Коршевнюк Л.О. Розділ 1. Основні положення систем підтримки прийняття рішень.

УДК 519.816

АНАЛИЗ ФОРМИРОВАНИЯ СОСТАВА ЭКСПЕРТНОЙ ГРУППЫ

Прокуда Элина Юрьевна[1]
ГВУЗ «Национальный горный университет», http://nmu.org.ua/, elinka9891@mail.ru[1]

В статье выполнен анализ формирования экспертной группы на примере оценки состояния базовых элементов карьерных автосамосвалов. Рассмотрена проблема подбора экспертов и представлен метод оценки компетентности экспертов.

Ключевые слова – оценка компетентности; эксперт; экспертная группа.

ВСТУПЛЕНИЕ

В последнее время из-за достаточно бурного развития науки и техники наиболее широко в управлении сложными системами стали использовать экспертные методы. Лицу, принимающему решение (ЛПР) для получения адекватных причин возникновения какой-либо проблемы необходимо сформировать экспертную рабочую группу [1]. При этом состав группы необходимо формировать из высококвалифицированных специалистов в конкретной области. Но проблема подбора экспертов является одной из наиболее сложных в теории и практике экспертных исследований. Рассмотрим и изучим данную проблему.

РЕШЕНИЕ ПОСТАВЛЕННОЙ ЗАДАЧИ

Выбор состава экспертной группы необходимо рассматривать с помощью многоэтапного процесса:

Этап 1. Определение экспертной области, а также цели экспертного оценивания.

Этап 2. Выбор количества экспертов в состав рабочей группы.

Этап 3. Составление списка возможных кандидатов в эксперты.

Этап 4. Формирование предварительного списка экспертной рабочей группы и оценивание уровня их компетентности.

Этап 5. Составление окончательного списка экспертной рабочей группы и оценивание уровня их компетентности.

Рассмотрим предложенные этапы более подробно и конкретно на примере оценки состояния базовых элементов карьерных автосамосвалов.

Этап 1. Определение экспертной области, а также цели экспертного оценивания.

ЛПР обычно определяет предметную область и цели исследования. Существуют различные цели экспертного оценивания:

1. Выбрать из множества предложенных альтернатив один, наиболее приемлемый.
2. Провести ранжирование предложенных альтернатив по степени их предпочтения.
3. Провести ранжирование и группировку альтернатив по степени их важности.
4. Сформировать набор факторов, провести их ранжирование, а также выбрать среди них наиболее значимые факторы, которые оказывают весомое влияние на итоговый показатель.

Также на данном этапе ЛПР необходимо определить задачу экспертного исследования и количество учитываемых факторов (или альтернатив). Рекомендуется брать не более 9-10 факторов, которые будут подлежать анализу и ранжированию, так как последующее увеличение факторов будет вести к сложности их ранжирования с учетом обеспечения согласованной оценки экспертов.

Применение экспертного метода предполагает соблюдения некоторых условий:

- экспертная оценка используется лишь в случае, когда нельзя решить вопрос другим более объективным методом;
- мнения экспертов должны быть независимыми;
- необходимо избавиться от факторов, которые могли бы влиять на искренность суждений экспертов;
- вопросы, предоставленные экспертам, должны быть точными и не подразумевать различное толкование;
- ответы экспертов должны быть однозначными и обеспечивать возможность их математической обработки.

Этап 2. Выбор количества экспертов в состав рабочей группы.

Количество экспертов в рабочей группе играет весомую роль, ведь с увеличением количества экспертов увеличивается точность исследования. Рассмотрим некоторые подходы для определения количества экспертов входящих в состав рабочей группы:

1. Количество экспертов m определяется по формуле (1):

$$m \geq 0,5 \cdot \left(\frac{1}{3b} + 5 \right), \qquad (1)$$

где b – ошибка результата экспертного анализа $0 < b < 1$. Принимая допустимую ошибку 5% ($b = 0,05$) в состав рабочей группы должно входит не менее 6 человек.

2. Согласно принципу Генштальта количество экспертов должно быть в пределах 10 человек, так как при большем количество экспертов довольно сложно согласовать их мнения, а также возможны проблемы с организацией работы экспертной группы.

3. Основываясь на результатах практической деятельности [2], рекомендуется в экспертную группу

брать не менее 7 и не более 25 экспертов, ведь малое количество экспертов, возможно, приведет к недостоверности работы группы, а большое – к сложности проведения экспертного опроса.

Этап 3. Составление списка возможных кандидатов в эксперты.

Формирование базового списка экспертов, которые возможно будут принимать участие в экспертном оценивании, рекомендуется производить ЛПР и его подчиненным. Необходимо создать полные списки специалистов по выбранной ранее исследуемой области. Так сформируется базовый список кандидатов в экспертную группу.

Этап 4. Формирование предварительного списка экспертной рабочей группы и оценивание уровня их компетентности.

Предварительный список формируется на основании базового списка. Первым проверяется возможность эксперта принять участие в работе группы в конкретное время. Затем происходит оценивание уровня компетентности экспертов. Для этого необходимо разработать критерии оценивания экспертов. В этот перечень следует внести:

1. Область исследования. Для успешной работы экспертной группы в целом каждый эксперт должен специализироваться на конкретной исследуемой области или смежной с ней.

2. Стаж работы и уровень профессиональной подготовки. Чем больше стаж работы, тем больше конкретных знаний и умений у специалиста и выше уровень подготовки такого эксперта.

3. Источник обоснования мнения эксперта. Чаще всего в данную категорию относят следующие критерии:

- проведенный теоретический анализ;
- производственный опыт;
- синтез печатных работ (как и отечественных, так и зарубежных);
- интуиция.

4. Личные качества. К основным требуемым личным качествам экспертов можно отнести:

1) Стремление к получению новых знаний, к повышению квалификации, к профессиональному росту.

2) Умение мгновенно оценивать сложившуюся ситуацию и находить эффективные решения проблемы.

3) Умение своевременно реализовывать принятые ранее решения.

4) Способность работы в коллективе (коммуникабельность).

5) Стрессоустойчивость.

6) Дисциплинированность и организованность.

7) Объективность.

8) Обладание логическим мышлением.

9) Аналитический склад ума.

10) Креативность.

Каждый эксперт рабочей группы должен владеть перечисленными выше качествами для успешной работы и получения желаемого результата исследования [3].

5. Опыт работы экспертом. Желательно чтобы специалист уже участвовал в подобных исследованиях в качестве эксперта.

6. Наличие публикаций в высокорейтинговых зарубежных и отечественных изданиях по профилю в течение последних трех лет.

7. Участие в симпозиумах, конференциях, семинарах. Высококвалифицированный специалист должен участвовать в различных симпозиумах, конференциях и семинарах, причем не только отраслевых, но еще и международных.

8. Наличие патентов, изобретений.

9. Оценка компетентности эксперта его коллегами или руководством. Данная оценка поможет скорректировать уровень компетентности эксперта.

По каждому критерию необходимо разработать свою шкалу оценивания. Также каждому критерию необходимо дать весовой коэффициент, так как каждый критерий для ЛПР более или менее важен. Проведя такое оценивания мы получим уровень компетентности K_i каждого i-го эксперта из предварительного списка экспертов. Необходимо проранжировать список уровня компетентности по убыванию.

Этап 5. Составление окончательного списка экспертной рабочей группы и оценивание уровня их компетентности.

Основываясь выбранном на Этапе 2 количестве экспертов, мы из предварительного списка отбираем необходимое их количество для проведения предполагаемого исследования.

Уровень компетентности рабочей группы определяется с помощью коэффициента представительности или компетентности экспертной группы. Данный коэффициент вычисляется по следующей формуле (2):

$$M = \frac{1}{m}\sum_{i=1}^{m} K_i , \qquad (2)$$

где K_i – коэффициент компетентности i-го эксперта.

ВЫВОДЫ

Экспертная группа, сформированная предложенным многоэтапным процессом выбора количественного и качественного состава, будет являться компетентной и способной решать поставленные перед ней задачи, если уровень ее общей компетентности будет находиться в интервале $0,7 \le M \le 1$. Предложенный метод оценивания экспертов будет применен к оценки состояния базовых элементов карьерных автосамосвалов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Орлов А.И. Эконометрика. Учебное пособие. - М.: Изд-во "Экзамен", 2002.

2. Горбашко Е.А. Управление качеством. – Спб.: Питер. 2008. – 384 с.

3. Михненко П.Ю. Секреты эффективных бизнес-решений. – М. NT Press. – 2007. – 288 с.

УДК 004.73

ИССЛЕДОВАНИЕ ФИЗИЧЕСКИХ ПРОЦЕССОВ В ИНФОРМАЦИОННЫХ СЕТЯХ

Дужая А.С., Магро В.И.
Научный руководитель: канд. физ.-мат. наук, доц. Магро В.И.
Днепропетровский национальный университет, Украина
E-mail: magrov@i.ua

Рассмотрены физические процессы при распространении сигнала в информационных сетях. Рассмотрены основные типы соединений. Приведены результаты расчета времени прохождения сигнала в таких соединениях.

Ключевые слова - Информационная сеть, коммутация пакетов, Ping, ICMP-Echo, задержка пакетов.

ВВЕДЕНИЕ

В настоящее время происходит сочетание локальных и глобальных информационных сетей. Услуги сети не всегда соответствуют современным требованиям, в связи с ограниченными возможностями ее транспортной инфраструктуры. Развитие инфокоммуникационных услуг требует решения задач эффективного управления информационными ресурсами с расширением функциональности сетей связи. Данные задачи могут быть решены путем математического моделирования физических процессов в информационных сетях. В докладе рассмотрены математические модели основных типов соединений.

ОСНОВНАЯ ЧАСТЬ

Рассмотрим локальную сеть, которая состоит из двух маршрутизаторов, соединенных между собой информационной сетью. В таких сетях можно легко исследовать потерю пакетов. Для этого будем использовать запрос ICMP-Echo или Ping. Этот запрос позволяет проверять соединения в сетях на основе TCP/IP протокола. Для исследования физических процессов распространения сигнала будем отправлять запрос (ICMP Echo-Request) на указанный узел сети, и фиксировать ответ, который приходит от него (ICMP Echo - Reply). Время между отправкой запроса и получением ответа (RTT, от англ. Round Trip Time) позволяет определять двусторонние задержки по маршруту и частоту потери пакетов, то есть определять загруженность на каналах передачи данных и промежуточных устройствах. Обычный запрос имеет длину 64 байта. По стандартам RFC 791 IPv4 суммарный объем пакета не может превышать 65 535 байт. Полное отсутствие ICMP - ответов может также означать, что удаленный узел (или какой-либо из промежуточных маршрутизаторов) блокирует ICMP Echo -Reply или игнорирует ICMP Echo - Request. С помощью ICMP Echo можно измерить время отклика маршрутизатора Cisco , имеющий свой IP - адрес, и любого устройства, который тоже имеет IP - адрес. Из рисунка 1 видно, что ICMP Echo-запрос можно отправлять как на любое устройство, который имеет IP-адрес, так и на другие маршрутизаторы. Отправим ICMP Echo-запрос с одного маршрутизатора на IP-адрес другого маршрутизатора. Для этого в пакете GNS3 используем следующий алгоритм:

- **configure terminal**
- **ip sla** *номер запроса*
- **icmp-echo** {*целевой-ip-адрес*} [**ip-адрес получателя**]
- **end**

Данный алгоритм позволяет исследовать прохождение сигнала с учетом загруженности сети в течение суток. Результатом такого моделирования являются данные, которые свидетельствуют о задержке пакетов, в связи с образованием очереди в сети. Этими данными являются:

- Полоса пропускания (*Bandwidth*), описывает номинальную пропускную способность среды передачи информации, определяет ширину канала. Измеряется в bit/s (bps), kbit/s (Kbps), Mbit/s (Mbps), Gbit/s (Gbps).
- Задержка при передаче пакета (*Delay*), измеряется в миллисекундах.
- Колебания (дрожание) задержки при передаче пакетов — джиттер.
- Потеря пакетов (*Packet loss*). Определяет количество пакетов, потерянных в сети во время передачи.

Этими параметрами определяется качество связи QoS. Этим термином в области компьютерных сетей называют вероятность того, что сеть связи соответствует заданному соглашению о трафике, или же, в ряде случаев, неформальное обозначение вероятности прохождения пакета между двумя точками сети. Если две подсети соединены каналом с невысокой пропускной способностью, например телефонной линией, то может возникнуть ситуация, в которой передача данных по сети будет сопровождаться дополнительной задержкой.

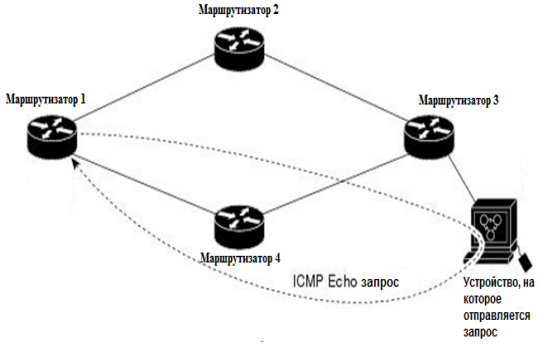

Рис. 1 – Схема отправки ICMP Echo запроса

Это связано с тем, что скорость подключения к сети конечных станций намного превышает скорость канала связи между подсетями, в результате чего канал связи становится узким местом данной сети. Это происходит только при использовании протокола TCP, ориентированного на соединение.

Если узел-приемник, подключенный к сети с достаточно высокой скоростью, например 100 Мб/с Ethernet, находится за компьютером под управлением Windows XP, на котором запущена служба общего доступа к подключению Интернета (ICS), и сервер, обменивающийся данными с узлом-приемником, также подключен к сети с достаточно высокой пропускной способностью и находится за узлом удаленного доступа, то возникает описанная выше проблема. В этом случае, исходя из скорости локальной сети узла-приемника, на узле-приемнике устанавливается большой размер окна приема. Узел-отправитель начинает передачу, используя сравнительно малый размер окна, но, если при передаче отсутствуют ошибки, постепенно увеличивает размер окна. Это может повлиять на производительность остальных подключений, существующих в данной сети и использующих протокол TCP. Их пакеты вынуждены будут долго находиться в очереди, ожидая отправки по медленному каналу связи. Если при передаче происходит ошибка, то данные передаются повторно, еще более загружая канал связи.

Чтобы избежать подобной ситуации, необходимо, чтобы компьютер, который находится на границе подсети и на котором запущена служба общего доступа к подключению Интернета, автоматически уменьшал размер окна передачи в соответствии со скоростью канала связи меньшей производительности, переопределяя при этом параметры, указанные приемником. Это позволит увеличить производительность, поскольку размер окна будет устанавливаться, таким образом, как если бы узел-приемник был подключен непосредственно к медленному каналу связи. Подобное регулирование размеров окна осуществляется планировщиком QoS-пакетов, выполняющимся на компьютере, на котором запущена служба общего доступа к подключению Интернета.

Многие пользователи подключаются к Интернету, используя достаточно медленные каналы связи (например, 56 Кб/с). Несмотря на небольшую скорость, многие пользователи зачастую одновременно запускают несколько программ, обращающихся к сети. К примеру, пользователи могут запустить программы загрузки файлов, работы с электронной почтой или программы интерактивного общения, а также программы для воспроизведения аудио- или видеозаписей. Почти все подобные программы используют в качестве транспортного протокола протокол TCP и открывают одно или несколько подключений.

Программа, обращающаяся к каналу первой, получает преимущество использования, пока подключение не достигнет устойчивого состояния. При этом появится возможность использования при обмене данными окна TCP максимального размера. Если запустится еще одна подобная программа, то будет использоваться алгоритм, ограничивающий объем данных, которые могут быть переданы без подтверждения приема. Поскольку пропускная способность канала частично используется первой программой, то второй программе потребуется больше времени для достижения устойчивого состояния, в результате чего передача будет вестись с меньшей скоростью.

Windows XP применяет алгоритм DRR (Deficit Round Robin), если операционная система использует медленный канал связи. Использование данного алгоритма возможно и в Windows 2000, но в Windows XP при работе с медленными каналами связи он используется по умолчанию. При этом выделяются несколько потоков данных, которым ставятся в соответствие потоки данных приложений. Эти потоки данных автоматически обслуживаются на циклической основе, что улучшает время реакции и производительность сетевых соединений, не требуя от пользователя изменения параметров вручную.

ЗАКЛЮЧЕНИЕ

Установлено, что увеличение времени передачи и возврата пакета зависит от нагрузки сети. При увеличении количества запросов с одного маршрутизатора на другой может образоваться очередь в сети, что приведет к задержке данных и неправильному распределению ресурсов локальной сети.

СПИСОК ЛИТЕРАТУРЫ

1. Cisco IOS IP SLAs Configuration Guide/2008. — 156 с.
2. Хилл Брайан. Полный справочник по Cisco / Брайан Хилл // Издательский дом «Вильямс». —2004

УДК 004.02

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМАХ ДИСТАНЦІЙНОЇ ОСВІТИ

Кручініна Євгенія Олександрівна,
Науковий керівник: д.т.н., проф. Алексєєв Михайло Олександрович
Державний ВНЗ «Національний гірничий університет», http://www.nmu.org.ua,
charlieinfinity13@gmail.com

Висвітлення причини актуальності питання дистанційної освіти та причин її розповсюдження и розвитку. Розглядаються технології, які стоять за розвитком цього напрямку, їх особливості

використання. Акцентовано увагу на важливості проблеми зберігання офіційної документації в електронному вигляді, визначено середовища і вимоги до організації інформації у такому вигляді. Охарактеризовано способи якісного захисту інформації.

Ключові слова: інформаційні технології, дистанційна освіта, принципи, база даних,безпека інформації.

ВСТУП

У час стрімкого розвитку технологій та все більшого використання Інтернет простору в усіх можливих сферах життя, постає питання про доцільність його використання для розширення можливостей доступу до тих чи інших ресурсів. Під ресурсами маються на увазі не тільки величезні обсяги інформації, але й ряд послуг та можливостей, які можуть стати доступними у будь-якій точці земної кулі. Так, одним із найважливіших напрямків є системи дистанційного отримання освіти. Звичайна бібліотека дедалі більше мігрує в електронну, а звичайні аудиторії замінюються віртуальними. Нові системи дистанційної освіти (надалі ДО) дедалі більше задовольняють потреби студентів та викладачів. Одержати ДО можуть люди, які не мають можливості сполучити роботу з навчанням або навіть одержати освіту за кордоном при мінімальних витратах, при цьому спектр вибору спеціальностей є дуже широким. Згідно з проведеними дослідженнями, в Україні вже 30%[1] навчальних закладів заявили про введення у систему освіти дистанційну форму навчання.

ПРИНЦИПИ ТА ТЕХНОЛОГІЇ ДИСТАНЦІЙНОЇ СИСТЕМИ ОТРИМАННЯ ОСВІТИ

Головною метою ДО є надання можливості отримання якісних знань, набуття відповідних умінь та навичок з використанням інформаційно-комунікаційних технологій та відповідного програмного забезпечення. При розгляданні цього питання слід відокремити головні етапи у побудові системи. По-перше, це розроблення її принципів. Кажучи про системи дистанційної освіти, можна виділити такі з них:

- Орієнтація на суб’єкт навчання - предмет виступає як засіб розвитку здібностей та професійних потреб як студента, так і викладача; останній не тільки «веде» навчальний процес, але й забезпечує його результативність
- Дистанційні принципи – характеризують діяльність з формування оптимального сполучення форм курування пізнавальною діяльністю, індивідуальний підхід до створюваних інтелектуальних продуктів та регламенту навчання.
- Принципи відкритості – доступність комунікативного простору, відкритість та гнучкість навчання, інтерактивність.[2]

По-друге, при створені курсів для системи дистанційної освіти, треба звернути увагу на підготовку матеріалів та тем предметів, а також на кваліфікації викладачів. Аналіз освітніх електронних ресурсів показує, що вони мають наступну класифікацію: за функціональною ознакою їх можна віднести до навчальних видань, за формою подання вони належать до категорії електронних видань, за технологією створення вони є програмним продуктом [3]. Тому об'єднуючим атрибутом моніторингу якості матеріалу є вимога задоволення загальноприйнятим міжнародним стандартам, якими є IMS, SCORM

По-третє, важливим фактором забезпечення достатнього рівня якості системи ДО на етапі організації навчального процесу є обґрунтований та виважений вибір спеціалізованого програмного забезпечення для управління системи. Центральний елемент, навколо якого збираються учасники дистанційної освіти є платформа ДО. Вона використовується для підтримки ДО, і її метою є створення та управління педагогічним змістом, індивідуалізоване навчання та телетьюторат, воно включає засоби, необхідні для трьох основних користувачів – викладача, студента, адміністратора На сьогоднішній день існує велика кількість систем для організації ДН. Найбільш популярніші з них Moodle, Blackboard , WebCt, Microsoft Learning Gateway та багато інших. Кожна з цих програм має своє призначення і займає певну нішу в системі дистанційної освіти. Єдиним реально працюючим інструментом зворотного зв’язку в таких системах є електронна пошта.

Останнім і не менш важливим питанням є перевірка результатів навчання і подальше засвідчення рівня отриманих знань. В цьому випадку передбачається кілька можливих варіантів. Існує багато прикладів успішного дистанційного контролю навчання (TOEFL, TestDaF), в основі яких лежить принцип делегації відповідальності за проведення контрольних заходів людям, які можуть бути не спеціалістами з перевірюваної галузі, але мають засвідчувати правильність проведення процесу згідно з установленим регламентом. А саме, це є ідентифікація/аутентифікація користувача (того, хто проходить екзамен), з використанням ,наприклад, технології розпізнавання облич, тощо. І фінальною нотою є документоване підтвердження проходження курсів, тобто сертифікація результатів.

БАЗА ДАНИХ СЕРТИФІКАТІВ

Проблема збереження електронної інформації та забезпечення доступу до неї є одним із серйозних викликів бурхливо мінливого інформаційного середовища. Метою збереження електронної інформації є забезпечення довготривалої (або вічної) доступності цифрових матеріалів, із збереженням всіх смислових і функціональних характеристик вихідних матеріалів, можливостей пошуку та інтерпретації для подальшого доступу і використання. Така потреба виникає в умовах, коли необхідне підтвердження офіційного документа для певної установи, а можливості зв’язку обмежені або не гарантують безпеку.

То ж як один з варіантів вирішення проблеми може бути створення бази даних, яка містить у собі документи, що підтверджували б рівень знань або певну спеціалізацію - сертифікати. Приклади

успішної роботи такої системи на сьогоднішній день вже існують (TestProvider від Microsoft, сертифікати проходження практика від ZyXEL). Використання такої системи зберігання має бути інтуїтивно зрозумілим – при введені номера сертифікату видається документ з усією необхідною інформацією.

Сертифікати є електронними документами, тому мають цінність тоді і тільки тоді, коли вони [4]:

- повні;
- аутентичні;
- доступні;
- актуальні.

Електронні сертифікати містять персональні данні і тому є інформацією з обмеженим доступом (ІзОД). Згідно вимог закону України «Про захист інформації в автоматизованих системах», для забезпечення захисту ІзОД при обробці її в автоматизованій системі (АС) необхідно створити комплексну систему захисту інформації (КСЗІ) . Створення КСЗІ в АС виконуються у відповідності з НД ТЗІ 3.7-003 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Окремою задачею є формування вимог щодо забезпечення властивостей інформації: конфіденційності, цілісності та доступності. Ці вимоги задаються як перелік мінімально необхідних рівнів послуг, які повинен реалізовувати комплекс засобів захисту обчислювальної системи АС. Цей перелік представляє собою функціональний профіль захищеності. Враховуючи, що такі системи повинні забезпечувати можливість підключення віддалених користувачів через незахищені канали зв'язку, окремо слід обґрунтувати та сформулювати критерії конфіденційність при обміні, цілісність при обміні, автентифікація при обміні, автентифікація відправника, автентифікація отримувача. Безумовно, окремою здачею є юридичний супровід таких систем.

ВИСНОВКИ

Запровадження систем дистанційної освіти є актуальною задачею, яку не можливо без використання інформаційних систем і сучасних інформаційних технологій.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. http://novaosvita.com.ua/wp-content/uploads/2011/10/Mykolaiv_PEDAGOGY.pdf#page=86
2. Матеріали Першої Всеукраїнської науково-практичної заочної конференції «Актуальні проблеми педагогічної науки», 2011р.
3. Демкин В.П., Можаева Г.В. Классификация образовательных электронных изданий: основные принципы и критерии. – Томский государственный университет. – 2003, http://www.ido.tsu.ru/ss/?unit=214.
4. Конявский В.А., Техническая защита электронных документов в компьютерных системах.

УДК 004.42:537.312.8:537.291

АВТОМАТИЗАЦИЯ РАСЧЕТА УДЕЛЬНОГО ЗАРЯДА ЭЛЕКТРОНА МЕТОДОМ МАГНЕТРОНА

Олишевский Илья Геннадьевич

Научный руководитель: ст. преподаватель каф. физики Журавлев Михаил Александрович

Государственное ВУЗ «Национальный горный университет», nmu.org.ua, E-mail: olishevskiyi@ukr.net

Рассмотрена задача виртуального моделирования лабораторной работы по разделу общей физики «Электрика и магнетизм». Проведено численное определение удельного заряда электрона методом магнетрона.

Ключевые слова: виртуальная лабораторная работа, удельный заряд электрона, критическая сила тока соленоида, критическая магнитная индукция, магнетрон.

АКТУАЛЬНОСТЬ ТЕМЫ

Одним из важнейших направлений современной трансформации заочной формы обучения в дистанционную форму является разработка научно и методологически обоснованных мероприятий, которые позволят эффективно и быстро выполнять виртуальные индивидуальные работы. При изучении дисциплин большую роль играют лабораторные работы, которые позволяют закрепить теоретические знания, проанализировать базовые положения и получить практический опыт выполнения исследований. При этом возникает проблема самостоятельного освоения студентом учебного материала и успешного выполнения виртуальной лабораторной работы. Одним из путей решения этой проблемы является использование современных информационных технологий.

Таким образом, в связи с переходом на дистанционную форму обучения возникла необходимость разработки автоматизированного расчета, который позволяет выполнить виртуальную лабораторную работу, обеспечить высокую точность расчетов и сократить время их выполнения. Поэтому тема работы является важной и актуальной.

СВЯЗЬ РАБОТЫ С НАУЧНЫМИ И УЧЕБНЫМИ ПРОГРАММАМИ КАФЕДРЫ

Научно-исследовательская работа выполнена в соответствии с учебной программой подготовки

бакалавров по направлению «Электротехника и электротехнологии» по дисциплине «Общая физика».

ЦЕЛЬ И ЗАДАЧИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ

Целью научно-исследовательской работы является разработка программы по автоматизации расчета удельного заряда электрона методом магнетрона, которая позволяет выполнять виртуальную лабораторную работу.

Для достижения поставленной цели были решены следующие задачи:

1. осуществлен выбор среды программирования;
2. разработана программа для расчета удельного заряда электрона методом магнетрона;
3. обеспечен удобный для пользователя интерфейс;
4. проведены исследования зависимость силы анодного тока диода от величины силы тока соленоида;
5. определена величина критической силы тока соленоида;
6. обеспечено представление результатов расчетов в графическом виде;
7. проведена систематизация полученных результатов и их представление в виде отчета;
8. подготовлена электронная презентация работы.

МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ

Экспериментальное исследование зависимости силы анодного тока от изменения силы тока соленоида [1, 2]. Численное исследование удельного заряда электрона методом магнетрона с помощью программы, разработанной в среде Delphi [3, 4].

ОСНОВНОЙ МАТЕРИАЛ

Экспериментальное исследование зависимости силы анодного тока от изменения силы тока соленоида было проведено с помощью следующего оборудования: стандартная кассета ФПЕ-03, источник питания и миллиамперметр. Геометрические параметры магнетрона приведены в табл. 1.

Таблица 1. Исходные параметры оборудования

Название характеристики	Единицы измерения	Значение
Длина соленоида, L	мм	150
Диаметр соленоида, D	мм	85
Полное число витков, N		2700
Радиус катода, r_k	мм	0,1
Радиус анода, r_a	мм	1,22

Было проведено три серии экспериментов при значениях анодного напряжения U_a, равных 50 В, 40 В и 30 В, соответственно. В каждой серии опытов значение анодного напряжения было постоянным.

Полученные экспериментальным путем массивы данных были занесены в программный код, так как отсутствует аналитическая зависимость анодного тока диода от магнитного поля.

На этапе выполнения программы пользователь из предложенных вариантов выбирает значение анодного напряжения U_a, и после нажатия кнопки «Розрахунок» таблица заполняется экспериментальными данными и высвечивается кнопка «Побудова і звіт» (рис. 1).

При нажатии кнопки «Побудова і звіт» программа по экспериментальным данным строит график зависимости анодного тока от силы тока соленоида, проводит касательные к точкам перегиба и определяет критическое значение силы тока соленоида. После этого программа рассчитывает значения критической магнитной индукции и удельного заряда электрона и выводит результаты на экран вместе с поясняющими формулами.

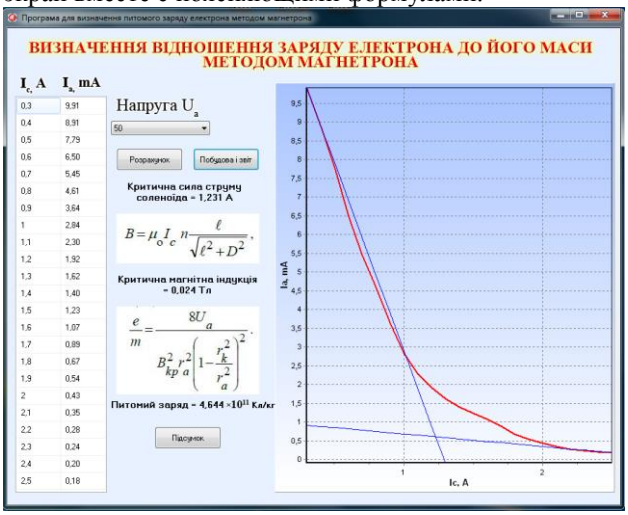

Рисунок 1. Главное окно программы

При изменении значения анодного напряжения обнуляются все данные в главном окне (рис. 1), и цикл расчета повторяется снова.

Результаты каждого цикла расчетов (с соответствующим значением анодного напряжения) заполняются в соответствующую строку итоговой таблицы окна результатов «Підсумок» и отображаются в графическом виде (рис. 2).

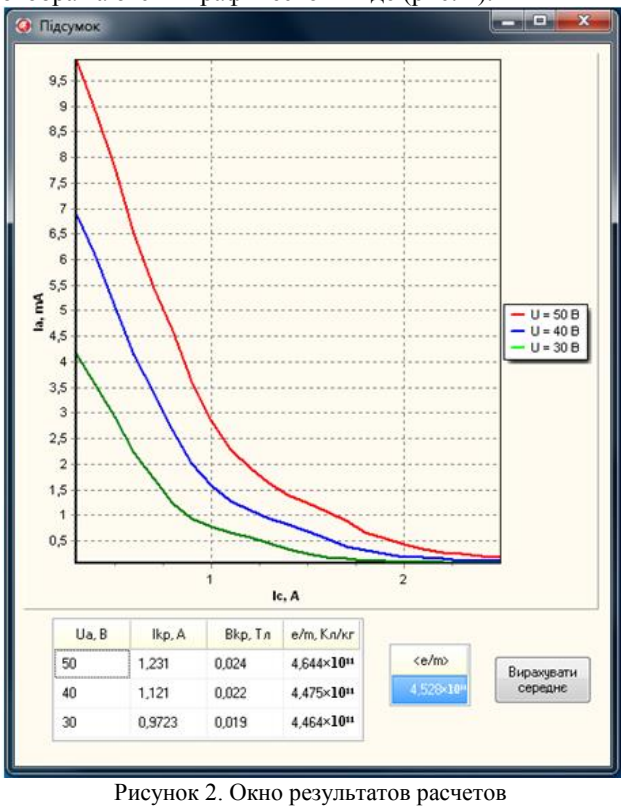

Рисунок 2. Окно результатов расчетов

После расчетов удельного заряда электрона для всех значений анодного напряжения в окне результатов появляется кнопка «Вирахувати середнє». Нажатие кнопки «Вирахувати середнє» приводит к расчету среднего значения удельного заряда электрона.

Достоинством разработанной программы является возможность представления результатов расчетов в графическом виде и в виде сводной таблицы (рис. 2). Наглядность представления результатов позволит студентам лучше понять суть изучаемого явления.

ВЫВОДЫ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Разработана программа, которая является современным программным продуктом, обеспечивающим выполнение виртуальной лабораторной работы по определению удельного заряда электрона методом магнетрона, точность полученных результатов и экономию времени проведения расчетов.

Отклонение результатов расчетов виртуальной лабораторной работы от результатов натурных экспериментов не превышает 3 %.

Программа представляет собой автономный исполняемый файл, что позволяет работать в ней без подключения к сети Интернет (в режиме офф-лайн). Этот момент важен для студентов дистанционной формы обучения, проживающих в небольших населенных пунктах с ограниченным или непостоянным доступом к сети Интернет.

В разработанной программе обеспечен понятный и удобный для пользователя интерфейс, который позволяет выполнить виртуальную лабораторную работу без затруднений пользователю любого уровня и сосредоточить внимание на изучении материала по дисциплине «Общая физика».

Методика автоматизации расчета удельного заряда электрона методом магнетрона будет внедрена в учебный процесс кафедры физики Государственного ВУЗ «Национальный горный университет» в 2014 году.

Материалы работы могут быть использованы студентами всех направлений подготовки при изучении дисциплины «Общая физика».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Електродинаміка. Частина ІІ. Матеріали методичного забезпечення дисципліни “Фізика” для студентів усіх спеціальностей / Л.І. Барташевська, А.С Зайцев, В.М. Мандрикевич, Т.В. Морозова, А.В.Чернай, – Д.: Національний гірничий університет, 2011.

2. Кучерук І.М. Загальний курс фізики / І.М. Кучерук, І.Т. Горбачук, П.П. Луцик. – К.: Техніка, 2001. – Т.2. – 290 с.

3. Кандзюба С.П. Deiphi 6. Основи програмування: Навчальний посібник / С.П. Кандзюба. Дніпропетровськ: УДХТУ, 2003. – 411 с.

4. Фаронов В.В. Deiphi. Программирование на языке высокого уровня: Учебник для вузов / В.В. Фаронов. – СПб.: Питер, 2003. – 640 с.

УДК 621.395

УСОВЕРШЕНСТВОВАНИЕ ПРОЦЕДУРЫ МЯГКОГО ХЭНДОВЕРА В СОТОВЫХ СЕТЯХ 3G

Чишкала А.П., Магро В.И.

ГВУЗ «Национальный Горный Университет», http://bit.nmu.org.ua/, e-mail: brat2mw@mail.ru

Предложено усовершенствовать процедуру мягкого хэндовера. Техническим результатом является сокращение расхода ресурсов и предотвращение ошибок маршрутизации трафика оборудования пользователя (UE). Результат достигается за счет того, что в процессе хэндовера UE целевая базовая станция не устанавливает ни один однонаправленный канал услуги локального подключения UE или не переадресует данные услуги локального подключения.

Ключевые слова – хэндовер, сеть 3G, мобильная связь, ошибки маршрутизации.

ВВЕДЕНИЕ

В системах подвижной сотовой связи важную роль играет метод автоматического переключения вызова на другой канал в момент, когда мобильная станция перемешается из соты в соту. Такой метод назвается хэндовер (от английского слова handover).

Хэндовер – это процедура передачи активного соединения между сотами [1, 2]. Это одна из ключевых процедур делающая сотовую связь любого стандарта (GSM, UMTS, LTE) истинно мобильным видом связи. Хэндовер позволяет абонентам не быть привязанным к какой-либо географической точке и дает возможность передвигаться в пределах сети оператора без разрыва соединения. Причиной хэндовера может быть не только перемещение абонента в пространстве, но и ухудшение качества сигнала от текущей базовой станции по каким-либо другим причинам. В частности, между абонентом и базовой станцией (БС) может возникнуть препятствие, ухудшиться метеоусловия, обслуживающая базовая станция или ее часть может выйти из строя и т.п.

Различают несколько видов хэндоверов (рис 1):

1. Передача соединения внутри соты (внутрисотовый хэндовер) предназначена для оптимизации нагрузки на соту или повышения качества соединения за счет смены несущей частоты BSC (Base Station Controller) контроллер базовых станци, а меняются только базовые станции.

2. Внутри одной БС между секторами – этот тип хэндовера происходит между двумя секторами одной БС.

3. Внутри одного BSC_между БС – в этом случае будут задействованы ресурсы уже нескольких сетевых элементов: BSC и двух БС, т.е. некоторое время может существовать два соединения между UE (User Equipment) и RNC (Radio Network Controller) через разные Node B (Узел B).

4. Между BSC внутри одного MSC (Mobile Switching Center) коммутатор мобильных сетей связи – в этом случае БС, между которыми происходит хэндовер подключены к разным BSC.

5. Между MSC – этот тип хэндовера выполняется когда БС подключены к разным MSC. В этом случае в новом MSC и устанавливается соединение до старого коммутатора, который получает название якорного MSC.

6. Между RAN (Radio access network) сеть радиодоступа– это так называемый межсистемный хэндовер. Он выполняется между базовыми станциями, относящимися к разным стандартам сотовой связи (GSM, UMTS, LTE).

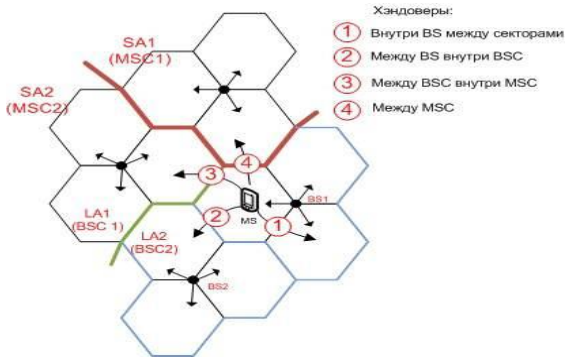

Рисунок 1. Различные виды хэндоверов.

В настоящее время развивается сетевая архитектура HNB (Home Node B). В данной архитектуре UE использует сеть доступа с авторизованным спектром и общим Интернет Протоколом (IP). Авторизованным спектром может быть спектр, используемый сетями беспроводного доступа, такими как UTRAN (Сеть Наземного Радиодоступа UMTS). В сетевой архитектуре HNB, HNB подключен к HNB GW (Home Node B Gateway), а HNB GW подключен к SGSN – (Serving GPRS Support Node) Обслуживающему Узлу Поддержки GPRS. Когда выполняется хэндовер UE от исходной базовой станции к целевой базовой станции, то исходная базовая станция явным образом передает информацию об однонаправленных каналах, которые заключают в себе переадресацию данных, целевой базовой станции посредством MME. Целевая базовая станция подготавливает ресурсы для всех однонаправленных каналов UE и однонаправленных каналов, которые заключают в себе переадресацию данных, и затем UE начинает хэндовер. Когда на UE существует услуга локального подключения, однонаправленный канал заново устанавливается на целевой базовой станции в процессе хэндовера. Однако услуга локального подключения не требует наличия непрерывности услуги, и установка заново однонаправленного канала на целевой базовой станции приводит к растрате ресурсов.

РЕЗУЛЬТАТ ИССЛЕДОВАНИЯ

Для преодоления указанных недостатков внесем изменения в способ хэндовера. Он включает в себя этапы, на которых получают информацию об однонаправленных каналах услуги локального подключения UE, если принято решение выполнить хэндовер UE; и выполняют хэндовер UE от исходного HNB к целевой базовой станции в соответствии с информацией об однонаправленных каналах услуги локального подключения. При этом целевая базовая станция не устанавливает ни один однонаправленный канал услуги локального подключения. Исходный HNB, в котором размещается UE, принимает решение о том, инициировать ли хэндовер UE, в соответствии с отчетом измерения в отношении целевой базовой станции, передаваемым от UE. Как правило, информация об однонаправленных каналах услуги локального подключения UE управляется MME (Mobility Management Entity), и MME может запросить локально хранящуюся информацию об однонаправленном канале для того, чтобы выяснить, какие однонаправленные каналы UE являются однонаправленными каналами услуги локального подключения, и получить информацию об однонаправленных каналах услуги локального подключения UE. Узел Б может получить информацию об однонаправленных каналах услуги локального подключения UE посредством MME.

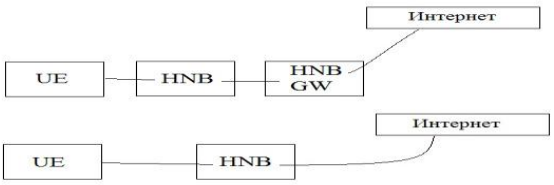

Рисунок 2. Услуга локального подключения доступа к Интернету

На рисунке 2 изображена услуга локального подключения UE. Она имеет два режима доступа: UE осуществляет доступ к Интернет посредством HNB или осуществляет доступ к Интернет посредством HNB и HNB GW.

Следующим этапом решения является то, что целевая базовая станция не устанавливает ни один однонаправленный канал услуги локального подключения при двух случаях. Первый случай, состоит в том, что, в то время как UE производит хэндовер от исходной базовой станции к целевой базовой станции, явное или неявное сообщение инструктирует целевую базовую станцию не устанавливать ни один однонаправленный канал услуги локального подключения, так чтобы не выполнять хэндовер однонаправленных каналов услуги локального подключения UE или не переадресовывать данные. Второй случай состоит в том, что сначала однонаправленные каналы услуги локального подключения UE высвобождаются, а затем UE осуществляет хэндовер от исходного HNB к целевой базовой станции, так что целевая базовая станция не устанавливает никакого однонаправленного канала услуги локального подключения UE, и тем самым избегают растраты ресурсов. Во втором случаи, суть состоит в том, что, когда все однонаправленные каналы UE являются однонаправленными каналами услуги локального подключения, то высвобождение однонаправленных каналов услуги локального подключения эквивалентно высвобождению всех однонаправленных каналов UE. Таким образом, не требуется выполнять хэндовер UE, и тем самым дополнительно избегают растраты ресурсов.

На рисунке 3 показан процесс осуществления хэндовера. Сообщение запроса прямого хэндовера, отправленное исходным MME, не несет в себе контекста однонаправленного канала услуги локального подключения UE.

Рисунок 3. Алгоритм осуществления хэндовера

Таким образом, показана возможность сокращения растраты ресурсов и предотвращения ошибок маршрутизации трафика UE. То есть предлагается следующее: если принято решение о хэндовере, то UE выполняет хэндовер от исходной базовой станции к целевой базовой станции в соответствии с информацией об однонаправленных каналах услуги локального подключения, при этом целевая базовая станция не устанавливает ни один однонаправленный канал услуги локального подключения; если принято решение инициировать хэндовер UE; и модуль хэндовера, сконфигурированный для хэндовера UE от исходной базовой станции к целевой базовой станции в соответствии с информацией, полученной модулем получения в отношении однонаправленных каналов услуги локального подключения, при этом целевая базовая станция не устанавливает ни один однонаправленный канал услуги локального подключения.

ВЫВОД

Предложено процесс хэндовера UE производить в соответствии с информацией об однонаправленных каналах услуги локального подключения UE. Следовательно время хэндовера целевая базовая станция не устанавливает ни один однонаправленный канал услуги локального подключения UE и не переадресует данные услуги локального подключения. Это экономит ресурсы и предотвращает ошибки маршрутизации пакетов услуги локального подключения.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАНОЙ ЛИТЕРАТУРЫ

1. Сотовая связь (Электрон. ресурс) URL: http://celnet.ru/HO.php

2. Берлин А. Н., Сотовые системы связи. М.: Эко-Трендз, 2007. –296 с.

УДК 621.396

ВИЗНАЧЕННЯ МІСЦЯ РОЗТАШУВАННЯ БАЗОВОЇ СТАНЦІЇ МОБІЛЬНОГО ЗВ'ЯЗКУ

Осадча Валентина Павлівна, Галушко Олег Михайлович
ДВНЗ «Національний гірничий університет» http://bit.nmu.org.ua/,
valia.osadchaya@yandex.ua, olegmih@i.ua

В статті розглянуто методику визначення оптимального місця розміщення базової станції мобільного зв'язку в умовах міської забудови. Наведені варіанти розміщення базових станцій. Виконано розрахунок щодо оптимального розташування базової станції в конкретних умовах.

Ключові слова – базова станція мобільного зв'язку; міська забудови; оптимальне розташування.

ВСТУП

Ефективне планування розміщення базових станцій (БС) є ключовою проблемою для оператора стільникового зв'язку як при розгортанні, так і при вдосконаленні мереж цього зв'язку. Це досить складна задача, повноцінного і закінченого рішення якої поки не існує, оскільки воно залежить від багатьох факторів різної природи. Тим не менш з позиції ефективності витрат на будування та експлуатацію мереж задача є вельми актуальною.

Серед факторів, які необхідно брати до уваги при розміщенні БС, ключовими є (окрім їх вартості) рельєф місцевості і щільність населення (потенціальних абонентів). Тому планування розміщень зводиться до мінімізації кількості БС, які максимально охоплюють необхідну зону покриття і максимально забезпечують доступ абонентів до мережі.

МЕТОДИКА РОЗРАХУНКУ

Для того щоб забезпечити зв'язок на всій ділянці, необхідно, щоб потужність сигналу від БС у кожному місці була б більше мінімально допустимої потужності, при якій мобільна станція (МС) зможе приймати сигнал мережі.

$$\min_{x,y \varepsilon G} P(x,y) \geq P_0;, \qquad (1)$$

де P_0 – мінімально допустима потужність сигналу, що приймається МС;

G – зона покриття мережі.

Беручи до уваги, що МС постійно проводить вимірювання рівнів сигналу на заданих оператором частотах для визначення стільники з найбільшим рівнем сигналу, потужність сигналу в точці (x,y), що приймається приймачем, залежить від відстані від МС до БС, за наступним законом:

$$P(x,y) = \max_i \frac{k_i}{(x-x_i)^2 + (y-y_i)^2}; \qquad (2)$$

де (x, y) – місце розташування МС; (x_i, y_i) – місце розташування і-ї БС;

κ_i – коефіцієнт послаблення сигналу для і-ї станції в точці (x, y).

Відстань від МС до і-ї БС:

$$R_i(x,y) = \sqrt{(x-x_i)^2 + (y-y_i)^2}; \qquad (3)$$

Таким чином, дана умова отримує геометричну інтерпретацію.

Варіанти можливого розташування БС для конкретних умов міської забудови наведені на рисунках 1, 2, 3 та 4 з вказанням рівня сигналів, отриманих за допомогою системи TEMS Investigation.

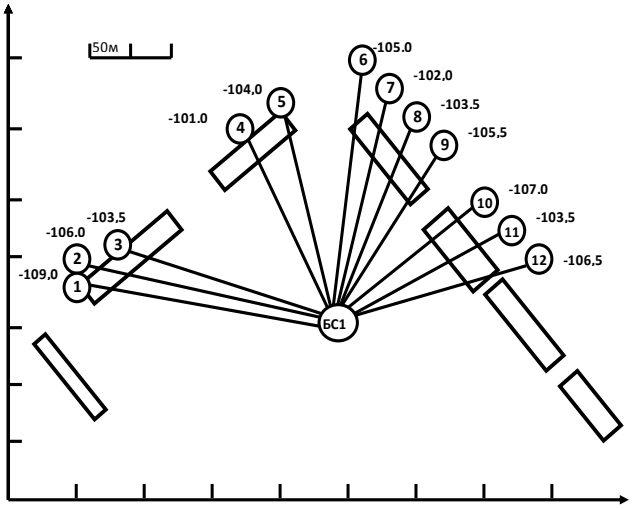

Рисунок 1. Перший варіант розташування БС

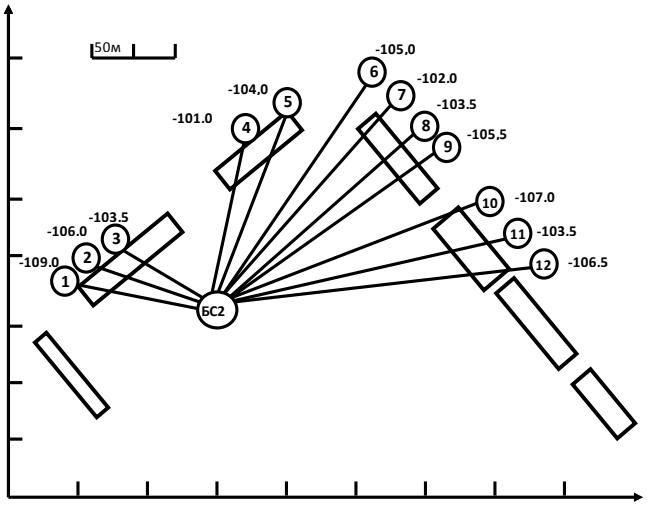

Рисунок 2. Другий варіант розташування БС

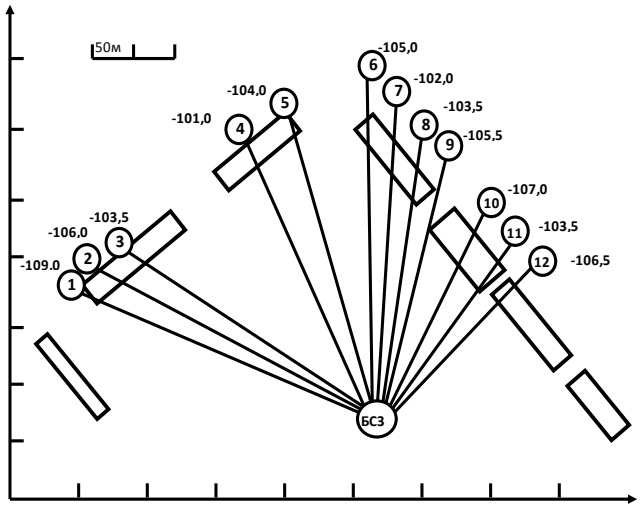

Рисунок 3. Третій варіант розташування БС

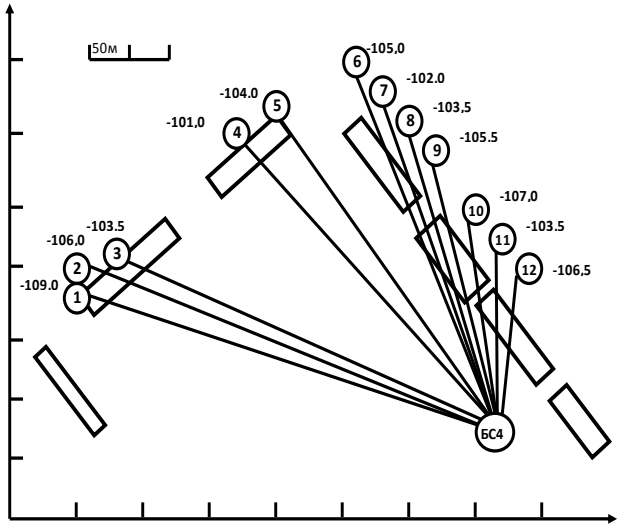

Рисунок 4. Четвертий варіант розташування БС

РЕЗУЛЬТАТИ РОЗРАХУНКУ

У таблиці 1 наведено результати розрахунків щодо визначення місця розташування БС за варіантом 2, при врахуванні положення точок їз визначеними потужностями сигналу (dBm).

За таблицями для кожного з можливих варіантів розташування базової станції побудовано діаграму сумарної відстані від БС - рисунок 5 до обраних точок з низьким рівнем сигналу у даному районі.

Рисунок 5. Діаграма сумарних відстаней від БС до обраних точок

Таблиця 1. Результати розрахунків щодо визначення місця розташування БС за варіантом 2.

i	Xi	Yi	Xbs-Xi	Ybs-Yi	(Xbs-Xi)^2	(Ybs-Yi)^2	(Xbs-Xi)^2 + (Ybs-Yi)^2	L
1	2	3	4	5	6	7	8	9
1	1,8	5,6	7,2	-1,1	51,8	1,21	53,05	7,28
2	2,2	6,1	6,8	-1,6	46,2	2,56	48,8	6,98
3	2,9	6,6	6,1	-2,1	37,2	4,41	41,62	6,45
4	6,4	9,5	2,6	-5	6,76	25	31,76	5,64
5	7,3	10,3	1,7	-5,8	2,89	33,6	36,53	6,04
6	9,9	11,3	-0,9	-6,8	0,81	46,2	47,05	6,86
7	10,5	10,6	-1,5	-6,1	2,25	37,2	39,46	6,28
8	11,2	9,8	-2,2	-5,3	4,84	28,1	32,93	5,74
9	11,7	9,3	-2,7	-4,8	7,29	23,1	30,33	5,51
10	12,8	7,7	-3,8	-3,2	14,4	10,2	24,68	4,97
11	13,5	6,9	-4,5	-2,4	20,3	5,76	26,01	5,1
12	14,3	6,1	-5,3	-1,6	28,1	2,56	30,65	5,54
Σ								72,39

ВИСНОВКИ

У роботі показано, що завдання оптимального розміщення БС зводиться до вирішення розглянутої задачі. За результатами аналізу розрахунків був вибраний другий варіант розміщення базової станції, який він має найменшу сумарну відстань зі всіх варіанів. Метод, що розглянуто, потребує подальшого аналізу для різних умов забудови.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Маковєєва М. М., Шинаков Ю. С. Системи зв'язку з рухомими об'єктами: Учб. посібник для вузів. -М.: Радіо і зв'язок, 2002. - 440 с.
2. Сундучков К. С., Мальчук М А., Кобзарь Л.С. Методика определения оптимальной топологии сети GSM для городского микрорайона. Наукові записки УНДІЗ, №6(8), 2008, ст.48-52.
3. Мухаджинов Р.Р. О постановке задачи выбора рационального размещения базовых станций сотовой связи./ Вестник Астраханского гос.техн.универс.,2008, №1, стр.127-129.

УДК 32.973.1

ЛАБОРАТОРНАЯ РАБОТА: МОДЕЛИРОВАНИЕ МОДЕМА V.32 BIS

Рыбина Яна Андреевна
Научный руководитель: к.ф.-м.н., доц. Гусев Александр Юрьевич
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua/ , E-mail: yana_rybina@mail.ru

Рассмотрены особенности протокола передачи данных V.32 bis, а также среда моделирования телефонного модема на основе протокола V.32 bis с описанием и схемой эмулятора телефонного канала.

Ключевые слова: – модем, эмулятор, телефонная линия, канал связи.

ВВЕДЕНИЕ

Одной из разновидностей систем связи, хорошо знакомых пользователям персональных компьютеров, представляют собой модемы [1].

Модем - это устройство, которое позволяет обмениваться данными по телефонной линии [2] . В сетевой среде модемы служат для соединения отдельных сетей между собой или между ЛВС (локально-вычислительной сетью) и остальным миром. Осуществлять связь непосредственно через телефонную линию компьютеры не могут, так как обмениваются данными, представленными в форме цифровых импульсов, а по телефонной линии можно передавать только аналоговые сигналы [3]. Главное назначение любого модема - обеспечение физической связи двух объектов, один из которых передаёт данные другому. Модулятор трансформирует сигнал перед началом передачи в соответствии с требованиями канала связи, а демодулятор на месте приёма производит обратную операцию, предоставляя информацию пользователю в удобном для восприятия виде [4].

МОДЕМ V.32 bis

Модем реализует квадратурный (QAM) модулятор и демодулятор со скоростью от 4800 до 14400 бит/с и разработан в соответствии с требованиями рекомендации ITU-T V.32 bis. Входным сигналом модема является последовательный битовый поток данных. Модем работает в полном дуплексе и использует эхоканселер для подавления отраженного эхо. Данный протокол обладает многими характерными чертами систем цифровой связи и благодаря своей простоте удобен для использования в учебных и демонстрационных целях.

Протокол позволяет легко изменять характеристики модема под имеющиеся аппаратные ресурсы. Так, ограничение максимальной задержки дальнего эха позволяет оптимизировать требования по памяти. Имеется модификация разработки, предназначенная для использования на 4-х проводных линиях и не использующая эхоподавитель [5].

Модем работает в двух режимах. Первый режим – передача данных. Модем принимает данные от компьютера, преобразует их в сигнал, посылает в телефонную линию и наоборот. Второй режим – командный. В этом режиме все данные, которые поступают в модем от компьютера, рассматриваются как команды, которые следует выполнить. Этот режим является для модема базовым и применяется для начальной инициации при включении, настройки параметров передачи данных и др. [2].

СРЕДА МОДЕЛИРОВАНИЯ

При моделировании модемов возникает необходимость в программной среде, обеспечивающей функционирование разрабатываемых программных структур модемов в удобном для отладки и тестирования режиме. Функционально, среда разработки состоит из следующих элементов: двух датапамп (софт модемов), эмулятора телефонного канала, источника и анализатора передаваемых данных, парсера скриптов конфигурирования среды, средств сохранения входных/выходных данных/отсчетов, журнала тестирования и т.д.

Данная тестовая среда использовалась для моделирования модема V.32bis. Среда разработки собрана на ПК под MS Visual C 2008 Express и на DSP Texas Instruments семейства 55XX под Code Composer Studio 3.3. Код оптимизирован на уровне языка С с использованием intrinsic и pragma и алгоритмической оптимизации. С минимальными переделками, код может использоваться на платформах DSP Texas Instruments семейства 64XX и 54XX.

ФУНКЦИОНАЛЬНЫЕ БЛОКИ СРЕДЫ

Среда моделирования предназначена для разработки и исследования полнодуплексных модемов и включает два вида программных модемов, один из которых работает как вызываемый, другой как вызывающий. Среда обеспечивает создание, конфигурирование, получение текущего состояния модемов и другие необходимые функции управления модемами. Принимаемые и передаваемые данные запрашиваются модемом с помощью функции обратного звонка. Эта же функция вызывается модемом для информирования тестовой среды или главного компьютера о изменениях состояния модема. Предполагается, что модем имеет интерфейс схожий с программным обеспечением Texas Instruments XDAS, для обеспечения независимости среды разработки от конкретного типа модема. Обращения к модему выполняются посредством программы согласования обмена.

Эмулятор телефонного канала предназначен для

моделирования искажений сигнала, возникающих при работе модемов через телефонную линию, функциональная схема которого приведена на рис.1.

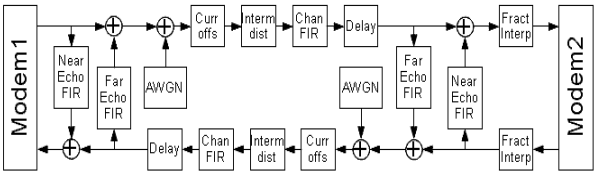

Рисунок 1 – Схема эмулятора канала

Модель канала симметрична, в том смысле что одинаковый алгоритм и общие параметры используются для симуляции искажений сигнала от модема 1 к модему 2 и в обратном направлении.

В качестве источника и приемника передаваемых модемами данных используется BER тестер, который показывает общее количество принятых бит, количество ошибочных бит, число потерь синхронизации и количество потерянных бит, принятых во время потери синхронизации.

Конфигурирование среды разработки и запуск тестов выполняется с помощью текстовых команд, читаемых из файла. Командный файл состоит из одного или нескольких тестов, каждый тест обеспечивает работу модемов в течении определенного времени или пока не будет передано заданное количество бит. Перед началом каждого теста все внутренние данные среды переинициализируются. В качестве конфигурации по умолчанию берется конфигурация предыдущего теста.

Таким образом команды делятся на два типа: команды устанавливающие параметры среды и команды запускающие тесты. Команды конфигурирования задают параметры самой тестовой среды, эмулятора канала или модемов [6].

ВЫВОДЫ

Данный пример является демонстрационным и не реализует ряда функций, необходимых в реальной системе цифровой связи. К таким функциям относятся адаптивная фильтрация для компенсации искажений, вносимых каналом связи, временная синхронизация, передача служебных сигналов для установления соединения и т. п.

На примере модема V.32 bis продемонстрирована возможность моделирования работы двух модемов, на базе стандартного программного обеспечения. Для моделирования работы приемника и передатчика рассмотренного модема можно также использовать программное обеспечение MATLAB, который поддерживает пакет Simulink с необходимыми настройками и инструментами.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Сергиенко А.Б. Пример использования пакета Communications - моделирование модема V.32bis Электрон. ресурс) / Способ доступа URL: http://matlab.exponenta.ru/communication/book5/index.php

2. Модемы. Технологии. Связь (Электрон. ресурс) / Способ доступа URL: http://v90.kiev.ua/articles/ - Загол. с экрана;

3. Как устроен и работает модем (Электрон. ресурс) / Способ доступа URL: http://www.woodwolf.ru/156/ ;

4. Поэтому.Ру: Ежедневное издание для всех любознательных (Электрон. ресурс) / Способ доступа URL: http://www.poetomu.ru/publ/zhurnal/tekhnika/kak_rabotaet_modem/31-1-0-162 - Загол. с экрана;

5. Лагутенко О.И. Современные модемы, 2002. – 346 с;

6. Power DSP. Среда разработки телефонных модемов. Описание среды разработки (Электрон. ресурс) / Способ доступа URL: http://powerdsp.narod.ru/modem_v32.html

УДК 004.77

НОВИЙ ПІДХІД ДО АНАЛІЗУ КОМУТОВАНИХ МЕРЕЖ З ГЕТЕРОГЕННОЮ СТРУКТУРОЮ

Марченко Віталій Анатолійович[1]
[1]Національний університет харчових технологій, http://nuft.edu.ua, vmarchenko@gmail.com

В доповіді розглядається підхід до аналізу сучасних комутованих мереж з гетерогенною структурою. Наведено особливості практичного застосування описаних методів при моделюванні комутованих мереж за допомого комплексу OMNET++.

Ключові слова – комп'ютерні мережі; rh-оптимізація; моделювання.

ВСТУП

Сучасні телекомунікаційні мережі являють собою складні системи з гетерогенною структурою. Тому дослідження різних аспектів їх функціонування представляє собою досить складну прикладну задачу. Базовим підходом до вирішення цієї проблеми є застосування різних моделюючих комплексів для дослідження необхідних аспектів функціонування.

Існує безліч різних систем моделювання телекомунікаційних мереж, але їх поєднує ряд особливостей функціонування. До них відноситься:

- дискретність процесів, що моделюються у середині системи;
- обмежений набір кількісних характеристик для аналізу користувачем (час, обсяг даних і т.п.).

Так у комплексі для моделювання OMNET++[1] у якості результатів моделювання заданої мережі дослідник одержує час проходження пакета через різні пристрої й ряд супутніх статистичних характеристик (загублені пакети, кількість повторних передач і т.п.).

Для більш комплексного дослідження необхідно використовувати додаткові моделі й методи, які дозволяють аналізувати функціонуючу систему в різних аспектах. Застосування методів rh-оптимізації[2] дозволяє досліджувати змодельовану телекомунікаційну мережу як єдину системі, що складається з набору буферів між якими передаються дані(що, по-суті, і представляє сучасна мережа з комутацією пакетів). Тоді продуктивність операції заповнення буфера визначається у відносних одиницях часу – байт-такт. Один байт-такт відповідає часу виконання однієї операції PUSH або POP (час прийому до буфера одного байта інформації). І якщо пакет містить D байтів, то час передачі (приймання) цього пакета з (в) буферу рівно D байт-тактам. При цьому всі накладні витрати, які з'являються в системі при передачі корисної інформації від джерела до одержувача, будуть визначатися довжиною заголовка (h). Тоді основними параметрами транспортного середовища з комутацією пакетів в загальному випадку будуть:

- кількість комутаторів (r) через які проходять данні, що передаються в межах сеансу зв'язку;
- обсяг корисних даних (D), що передаються від відправника до отримувача;
- довжина заголовка (h) як мірило всіх накладних витрат, що утворюються при передачі корисних даних.

При цьому загальний час передачі буде визначатися за формулою(1)

$$T_{A\to B}^{D} = D\,(r+1) + \sum_{i=1}^{r+1} h_i \quad (1)$$

Перевагою застосування цих методів для аналізу функціонування мережі є можливість одержувати відносні кількісні оцінки функціонування різних частин мережі в незалежності від використаної топології, протоколу або налаштувань конкретної підмережі. При цьому досить просто порівнювати різні варіанти побудови й реалізація мережі або використовуваних мережних протоколів як єдиної системи передачі даних. Зокрема маючі дані про кількості комутаторів та об'єму даних інформації, що передається можна апріорі визначити мінімальний час доставки як

$$\min T_n^D = D + 2\sqrt{Dr\max\{h_i\}} - \max\{h_i\} + \sum_{i=1}^{r+1} h_i$$

Таким чином регулюючи розмір довжини заголовку можна отримати необхідний час доставки даних.

Але ключовою проблемою є те, що в результаті розрахунків виходять значення у відносних одиницях. У випадку використання цих методів у рамках єдиної конфігурації телекомунікаційної мережі, але з різними параметрами комунікаційних протоколів, ця проблема нівелюється. Але для різних моделей мережі часовий інтервал необхідний для виконання одиничної операції буде різним, що вимагає його розрахунків.

ВИСНОВКИ

У кінцевому результаті при проведенні моделювання для практичного використання необхідно одержати максимально точні часові характеристики мережі які можна верифікувати, як за допомогою моделюючого комплексу так і в рамках реально функціонуючої мережі. У доповіді описуються підходи до розв'язку цієї проблеми, а також показуються практичне їхнє застосування разом з моделюючим комплексом OMNET++.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. OMNeT++ Network Simulation Framework. www.omnetpp.org.

2. Алишов Н.І. Оптимізація комутації пакетів в розподілених системах // Комп'ютерні засоби, мережі та системи. — 2004. — No 3. — С.87 — 95.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. БЕЗПЕКА ТА ЗВ'ЯЗОК

VI ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
СТУДЕНТІВ, АСПІРАНТІВ, МОЛОДИХ ВЧЕНИХ

3 квітня 2014 р.

Підписано до друку 24.03.14. Формат 30 х 42/2.
Папір офсетний. Ризографія. Ум.друк.арк. 8,4
Обл.-вид.арк. 8,2. Тираж 50 прим. Зам. №

Підготовлено до друку у Державному ВНЗ
«Національний гірничий університет»
49005, м. Дніпропетровськ, просп. К. Маркса, 19

Надруковано у ТОВ «САЛВЕЙ»
Свідоцтво № 233689904636
49000, м. Дніпропетровськ, вул. ак. Чекмарьова, 10 / 7