КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

Наукові доповіді та тези учасників
науково-технічної конференції
12-13 березня 2015 року

Київ 2015

УДК 658:0005.922.1:33(082)
ББК 65.29-98.43

Редакційна колегія:

Анісімов І.О. — доктор фізико-математичних наук, професор (голова)
Оксіюк О.Г. — доктор технічних наук, професор (заступник голови)
Бурячок В.Л. — доктор технічних наук, професор
Довбня С.Я. —кандидат військових наук, доцент
Мачуський Є.А. — доктор технічних наук, професор
Рєзніков М.І. — кандидат технічних наук, доцент
Самохвалов Ю.Я. — доктор технічних наук, професор
Субач І.Ю. — доктор технічних наук, доцент
Толюпа С.В. — доктор технічних наук, професор
Юдін О.К. — доктор технічних наук, професор

Відповідальний редактор — *Довбня С.Я.*
Технічний редактор — *Четверіков І.О.*

Інформаційна безпека України: Зб. наук. доп. та тез науково-технічної конференції; м. Київ, 12-13 березня 2015р., Київський національний університет імені Тараса Шевченка / Редкол.: І.О. Анісімов (голова) та ін.. — К.: Київський національний університет імені Тараса Шевченка, 2015. — 156 с.

Збірник містіть тексти наукових доповідей та тез учасників науково-технічної конференції **«Інформаційна безпека України»**, що відбулася 12-13 березня 2015 р.

Тексти виступів і тез опубліковано в авторській редакції однією з робочих мов конференції: *українською, російською, англійською.*

Київський національний університет імені Тараса Шевченка, 2015

ЗМІСТ

ВСТУП..... 10

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

Гребенюк А.

Подходы к оценке защищенности периметра информационной системы предприятия 11

Довбня С.Я., Хлапонін Ю.І.

Науково-методичне забезпечення системи інформаційної безпеки держави 12

Козловський В.В., Хлапонін Ю. І., Міщенко А.В.

Нечіткі нейронні продукційні мережі в системах захисту інформації..... 14

Косогов О.М.

Концептуальні основи створення системи інформаційної безпеки у сфері оборони України 15

Мачуський Є.А.

Mystery of 137 prime or simplex quantum theory 16

Оксіюк О.Г., Кохановський О.І.

Вирішення питань щодо підготовки/підвищення кваліфікації фахівців у галузі інформаційної безпеки. Сучасний підхід 19

Прогонов Д.О., Яцура П.П., Кущ С.М.

Деструкция стеганограмм с данными, встроенными в области преобразования цифрових зображений 20

Самохвалов Ю.Я., Бурба О.И.

Планирование мероприятий по минимизации рисков информационной безопасности 21

Синицын И.П., Колтик М.А.

Анализ построения модепли угрози нарушителей информации с использованием онтологии создания и проведения испытаний КСЗИ..... 22

Соснін О.В.

Про потребу інноваційного оновлення сенсу проблем безпеки 25

Субач І.Ю., Васильєв О.Я

Візуалізація даних у системі виявлення кібернетичних атак..... 28

Толюпа С.В., Дружинін В.А.

Застосування теорії декомпозиції для оцінки ефективності безпеки інформаційних систем 29

Шевченко А.С.

Оцінка безпеки інформаційної інфраструктури військових систем радіозв’язку на етапі проектування з урахуванням функціонування в умовах впливу інформаційних атак 30

Юдін О.К., Бучик С.С.

Український сегмент дерева ідентифікаторів державних інформаційних ресурсів..... 35

НАУКОВО-ТЕХНІЧНІ ТА ПРАКТИЧНІ АСПЕКТИ РОЗРОБЛЕННЯ ТА ВИКОРИСТАННЯ ЗАСОБІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Баранник В.В., Комолов Д.И., Тарнополов Р.В., Отман Шади О.Ю.

Методология селективной защиты видеопотока по базовым кадрам для ведомственных систем 37

Вавдічик М.І.

Аналіз генератору шуму мереж живлення 38

Васильєва В.О., Розорінов Г.М., Чичикало Н.І.

Джерела виникнення похибки та оцінка ступеню їх впливу на характеристики радіоканалу..... 41

Власенко Я.Ю., Василенко О.Д.

Можливість використання модернізованих ПІЧ-детекторів у якості «Квазітепловізорів 42

Власенко М.Ю., Василенко О.Д.

Розширення можливостей двопозиційних радіопроменевих систем виявлення..... 45

Войтко В.В., Ільницький А.І.

Проблемні питання моніторингу джерел радіовипромінювання сучасних телекомунікаційних мереж та напрям їх вирішення 46

Воронкова Е.С., Фокин Д.Д.

Кожно-гальванические реакции в современных биометрических технологиях 47

Двухглавов Д.Э., Твердохлеб В.В., Ларин В.В., Мусиенко А.П.

Алгоритм сжатия видеопотока с использованием битового куба..... 48

Довбня С.Я., Шпильовий В.С., Нікольський С. А.

Обрання виду акустичного шуму для захисту комерційної інформації..... 50

Довбня С.Я., Солдатенко О.О., Підлипна Т.М.

Науково-методичне забезпечення створення та функціонування системи інформаційної безпеки держави 52

Довбня С.Я., Кошиченко А.В., Нікірін А.В., Седько В.О.

Аналіз використання узгоджених сигналів при проектуванні захищеної інформаційно-телекомунікаційної системі з безпілотними летальними апаратами..... 54

Евсеев С.П., Свердло Т.А.

Механизмы интегрованного обеспечения безопасности и достоверности даннях на основе крипто-кодовых систем..... 55

Жердєв М.К., Пампуха І.В., Жиров Г.Б.

Алгоритм шифрування інформації з використанням керованого, випадкового та нелінійного елемента генерації ключів..... 57

Запорожець Т.С.
Функціональна модель бази даних загроз безпеці державних інформаційних ресурсів 60
Zhivkov A.P., Frolov A.V.
THE MYSTERIOUS NUMBER 137 OF QED AND MODERN DAY MEANS OF INFORMATION SECURITY 61
Machusky E.A.
STAIRSING OF 137 PRIME AS A STAR SING OF NATURE 62
Міщенко В.О., Драглюк О.В.
Створення захищеного обміну голосовою інформацією з допомогою технологій VOIP та OPENVPN 63
Морозова А.Д.
Исследование метода ВЧ-навязывания в телефонной линии 64
Нужний С.М.
Нові напрямки в забезпеченні захищеності акустичної інформації 66
Рєзніков М.І., Петрик Д.О., Семенюк В.І.
Аналіз методів захисту інформації в мобільних мережах третього та четвертого покоління 67
Розорінов Г.М., Сидорков Н.А., Чичикало Н.І.
Радіочастотна ідентифікація рухливих об’єктів спеціалізованих приміщень 69
Розорінов Г.М., Фурса В.О., Чичикало Н.І.
Розробка інструменту для частотно-часового аналізу сигналів в середовищі графічного програмування LabVIEW 70
Розорінов Г.М., Чичикало Н.І., Бородін Д.Ю.
Розробка віртуального інструменту «Поширення радіохвиль» для дослідження радіо передавальної системи 72
Свіжевський В.Ф., Зінченко С.А.
Пасивна акустична система виявлення безпілотних літальних апаратів 74
Турти М.В.
Принципи вибору методу формування функцій належності для задач обробки нечітких даних в інформаційній безпеці 75
Шемшур А.О., Мелешко О.О.
Методи ідентифікації та встановлення автентичності 76
Щебланін Ю.М., Левковець Г.С.
Законодавчі та технічні аспекти передачі закритої інформації по відкритим каналам 78

МЕТОДИ, ЗАСОБИ І ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Баранник В.В., Рябуха Ю.Н., Подлесный С.А., Бекиров А.Э.

Анализ действия кибератак на видеоинформационный ресурс в информационно-телекомуникационных сетях 80

Безмалый Н.В.

Риски использования мобильных устройств 81

Блінцов О.В., Корицький В.І.

Захищена система інформаційного обміну судна-носія прив'язної підводної системи 83

Браіловський М.М.

Шляхи підвищення захищеності мереж за рахунок збільшення функціональної стійкості 86

Бурба О.І.

Стан забезпечення інформаційної безпеки проектів національної програми інформатизації за результатами їх науково-технічної експертизи 87

Бурба О.І., Пасічник О.О.

Сигнатурний підхід до моніторингу загроз інформаційної безпеці інформаційних систем на основі моделі OSI 89

Бурлаков В.М., Домрачев В.М., Третиник В.В.

Видобування інформації з даних (DATA MINING), кібербезпека та запобігання шахрайству 90

Гаврилюк Г.В.

Технології управління інформаційною безпекою 91

Гірік Ю.А.

Втрати від витоку інформації 93

Головко О.О., Новіков В.П.

Комплексна система захисту інформації на основі застосування FUZZY-технологій 94

Гончар С.Ф., Леоненко Г.П., Юдін О.Ю.

Забезпечення інформаційної безпеки об'єктів критичної інфраструктури України 95

Данчук В.Д., Ананченко О.Є., Ананченко В.Є.

Удосконалення методів забезпечення інформаційної безпеки корпоративних інформаційних систем 96

Довбня С.Я., Бурлаков В.М., Драний О.В.

Практичні аспекти створення комплексної системи захисту персональних даних в ІТС 98

Дудка М.П., Четверіков І.О.
Безпека в сучасних мережах IP телефонії 100
Єсіна М.В.
Методи та принципи автентифікації в електронній ідентифікації 102
Замула А.А.
Метод оптимизации выбора дискретных сложных сигналов в целях обеспечения информационной безопасности в многопользовательских телекоммуникационных системах..... 104
Замула А.А., Семенко Е.А.
Программный комплекс генерации и исследования дискретных последовательностей для приложений информационной безопасности в телекоммуникационных системах..... 105
Затарі А.
Промислове шпигунство 106
Зибін С.В.
Вимоги до експертної СППР по забезпеченню інформаційної безпеки підприємства..... 108
Исирова Е.В.
Бизнес модель информационной безопасности 109
Карпов А.Г.
Квантовий генератор випадкових чисел..... 110
Ковтун О.С., Гончаренко М.В., Щербина І.С.
Застосування теорії прийняття рішень при управління інфокомунікаційними мережами 111
Кравченко К. В.
Про інформаційну безпеку особистості..... 112
Курдеча В.В., Чирченкова М.А.
Защита SDR-термінала от воздействия вредоносного програмного обеспечения..... 114
Курченко О.А., Халапсіна О.А.
Технічні заходи у сфері забезпечення інформаційної безпеки на підприємстві..... 115
Кутовий М.В., Новіков В.П.
Модель системи менеджменту інцидентів інформаційної безпеки..... 117
Левченко О.В.
Методичний підхід до проведення інформаційних операцій 118
Лукова-Чуйко Н.В.
Моделювання оптимальних систем захисту інформації..... 119
Майстренко М.К.
Сучасні технології захисту карткових розрахунків..... 121

Мохор В.В., Цуркан В.В., Крук О.М.
Нормативно-правовий аспект розробляння системи менеджовування ризику безпеки інформації 122
В.В. Мохор, О.В. Цуркан, Р.П. Герасимов
Соціоінженерна загроза інформаційно-психологічній безпеці людини в кіберпросторі 123
Никифорук І.В., Мелешко О.О.
Оцінка зберігання даних в «хмарних» сервісах 124
Оксіюк О.Г., Вялкова В.І.
Політіка безпеки інформації операційної системи 126
Онацкий А.В.
Модификация пороговой схемы разделения секрета Блэкли 127
Пікуль О.І., Толюпа С.В.
Методи захисту інформації у мережах зв'язку 128
Плескач В.Л., Плескач М. В.
Інформаційна безпека України в умовах розбудови державності 129
Поліщук К.А.
Процесний підхід в управлінні інформаційною безпекою 131
Приступа В.В.
Концептуальні аспекти забезпечення інформаційної безпеки в банківській системі 132
Прогонов Д.А., Паничева Д.О., Дорошенко А.В.
Использование пакета тестов nist для определения области встраивания стегоданных в контейнер 134
Прогонов Д.А., Черепахова К.В., Чипак М.А.
Обнаружение и подавление сообщений, встроенных в контейнеры на основе LSB-методов 135
Прус Р.Б.
Аналіз уразливостей об'єктів захисту інформації 136
Рубан І.В., Лошаков Є.С.
Система протидії повільним dos-атакам 138
Самойленко Д. М.
Динамічний стегозахист мережного ресурсу 139
Скрипник В.В., Жураковський Б.Ю.
Інтелектуальний підхід до управління мережними відмовами систем передачі даних 140
Стойчев М.І., Новіков В.П.
Забезпечення інформаційної безпеки в інфокомунікаційних системах спеціального призначення на основі методу енергетично-ефективного перетворення ІКМ-сигналів 142

Темников В.А., Конфорович И.В.
Система внутрисменной голосовой аутентификации авиадиспетчеров в режиме реального времени 143
Terentiev O. M., Prosyankina-Zharova T. I.
MODELING of INFORMATION DISSEMINATION USING THE CELLULAR AUTOMATA 144
Толюпа С.В., Павлов І.М.
Моделювання процесів прийняття рішень при проектуванні систем захисту інформації..... 146
Фігура Д.Л., Новіков В.П.
Обґрунтування методів та засобів підвищення захищеності систем електронних платежів 147
Хорошко В.О., Хохлачова Ю.Є.
Захист інформації автоматизованих систем 148
Шестак Я.В., Оксиюк А.Г.
Обнаружение компьютерных атак на основе анализа данных мониторинга несколькими способами..... 150
Цепа Н.В., Наконечний В.С.
Розробка методики контролю стану каналу систем радіозв'язку при впливі навмисних завад 153
Юдін О. К., Зюбіна Р. В.
Концепція впровадження хмарних технологій в Україні 154

ВСТУП

Нині розвиток сучасних інформаційних технологій, під якими розуміються процеси, методи пошуку, збору, зберігання, обробки, представлення, розповсюдження інформації та способи здійснення таких процесів і методів, є одними з найважливіших складових національних інтересів в інформаційній сфері .

Однак, поряд з перевагами побудови інформаційного суспільства, збільшуються і ризики, пов'язані з існуванням загроз безпеки інформаційним і телекомунікаційним засобам і системам. Захист інформаційних ресурсів від несанкціонованого доступу, знімання інформації засобами технічних розвідок, забезпечення безпеки інформаційних і телекомунікаційних систем, також є одним з основних національних інтересів в інформаційній сфері .

У зв'язку з цим виникає необхідність розробки сучасних методів і систем захисту інформації від різних типів загроз у всіх перерахованих системах.

Досить велика кількість засобів і систем захисту інформації створюються на основі математичних моделей, з використанням методів цифрової обробки сигналів а також використовують у своїй роботі інтенсивні логічні обчислення.

В роботі конференції взяли участь:

- представники вищих навчальних закладів — Київського національного університету імені Тараса Шевченка, Національного технічного університету України «Київський політехнічний інститут», Національного авіаційного університету, Національного університету кораблебудування імені адмірала Макарова, Харківського національного університету радіоелектроніки, Харківського університету Повітряних Сил імені І.М. Кожедуба, Харківського національного економічного університету імені Семена Кузнеца, Харківського національного університету імені В.Н. Каразіна, Національного транспортного університету, Одеської національної академії зв’язку імені О.С. Попова, Державного університету телекомунікацій, Європейского університету, Військового інституту телекомунікацій та інформатизації, Інституту спеціального зв’язку та захисту інформації НТУУ «КПІ»;
- фахівці структурних підрозділів Адміністрації Держспецзв’язку України, Служби безпеки України, Служби зовнішньої розвідки України, Адміністрації Державної прикордонної служби України, Міністерства обороні України, Міністерства внутрішніх справ України, Управління державної охорони України, інших органів державної влади;
- спеціалісти організацій та установ Державного інституту науково-технічної та інноваційної експертизи, Державного науково-дослідного інституту Спецзв’язку, Інституту програмних систем НАН України, Інституту проблем моделювання в енергетиці ім.. Г.Є Пухова НАН України , ДП «Укртехінформ», ДП «Українські спеціальні системи», АТ «Ощадбанк», ПАТ «НДІ ЕМП», ПАТ «МАРС», ТОВ «НікС», ТОВ «D.A.S.», ТОВ «Криптон», НДЦ «Тезис» НТУУ «КПІ», ДП НАЕК «Енергоатом», ТОВ «Криптософт», ТОВ «Епос», ТОВ «Ріас», НВП «Плазмотехніка», ІТЦ «Хай-Тек-Бюро».

УДК 004.056.53

А. Гребенюк
Старший консультант по безопасности,
ИТЦ «Хай-Тек Бюро»

ПОДХОДЫ К ОЦЕНКЕ ЗАЩИЩЕННОСТИ ПЕРИМЕТРА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

За последние несколько лет информационные технологии не только значительно расширили возможности бизнеса, но и сделали его более уязвимым. С одной стороны, налаживая электронный обмен данными и документами с клиентами или партнерами через Интернет, компании делают свой бизнес эффективным, но с другой стороны, ставят его под угрозу. Неуязвимых систем не бывает. И нахождение злоумышленниками уязвимостей в корпоративной сети (например, ошибок в реализации сетевых сервисов и в настройках сетевого оборудования) может привести не только к прямому финансовому ущербу, но и к потере репутации, утрате конкурентных преимуществ и другим негативным последствиям. Огромное число успешных вторжений наглядно показывает незащищенность огромного числа ресурсов. Незащищенность внешних рубежей сети компании обычно обусловлена целым рядом факторов.

На первый взгляд, наиболее типовые факторы — это:

- непонимание менеджментом величины ущерба, который может принести успешная атака на ИТ систему компании;
- отсутствие информации у менеджмента об истинном уровне защиты; ложная уверенность менеджмента в надежности собственной защиты;
- отсутствие или нехватка квалифицированного персонала в отделе ИТ-безопасности;
- отсутствие разработанной стратегии и политики информационной безопасности; «мы не представляем интереса для атаки»; «в нашей вычислительной системе нет критично важной для компании
- информации»; «наш веб-сервер выполняет только представительскую функцию и его взлом не повлечет для компании значимого ущерба».

Компании, как правило, полагаются на существующие программные или аппаратные решения в безопасности. Они тратят множество средств на последние версии антивирусного ПО и дорогие аппаратные брандмауэры, не получая ничего помимо теоретических доказательств, что вложенные деньги делают их сети более защищенными от хакерских атак. Тестирование на проникновение (тесты на преодоление защиты, penetration testing, pentest, пентест) является популярной во всем мире услугой в области информационной безопасности. Более того, риски связанные с инсайдерами либо вообще не берутся во внимание, либо считаются несущественными.

Основная задача теста на проникновение — идентификация максимально возможного числа уязвимостей информационной системы (ИС) предприятия за ограниченное время при заданных условиях и текущем состоянии ИС, их

ранжирование и разработка предложений по снижению рисков, с ними связанных.

Тест на проникновение — обязательная и очень важная часть аудита информационной безопасности. Полноценный результат проведения теста возможен лишь в случае работы высококвалифицированных профессионалов, имеющих опыт оценки активного ответа системы в реальном времени.

УДК 621.321

С.Я. Довбня, к.в.н., доцент

Київський національний університет імені Тараса Шевченка

Ю.І. Хлапонін, к.т.н., с.н.с.

Національний авіаційний університет

НАУКОВО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Нині розвиток сучасних інформаційних технологій, під якими розуміються процеси, методи пошуку, збору, зберігання, обробки, представлення, розповсюдження інформації та способи здійснення таких процесів і методів, є одними з найважливіших складових національних інтересів в інформаційній сфері [1, 2].

Однак, поряд з перевагами побудови інформаційного суспільства, збільшуються і ризики, пов'язані з існуванням загроз безпеки інформаційним і телекомунікаційним засобам і системам. Захист інформаційних ресурсів від несанкціонованого доступу, знімання інформації засобами технічних розвідок, забезпечення безпеки інформаційних і телекомунікаційних систем, також є одним з основних національних інтересів в інформаційній сфері [2]. Для забезпечення безпеки інформації необхідно вирішити завдання забезпечення конфіденційності, цілісності та доступності.

В умовах розвитку інформаційного суспільства, з одного боку підвищуються обсяги інформації, що обробляється в інформаційних і телекомунікаційних системах, з іншого боку — збільшується і ймовірність ризиків, пов'язаних з існуванням загроз безпеки інформації. Про це свідчить збільшення частки надання державних послуг в електронному вигляді, розвиток системи ситуаційних центрів, повсюдне запровадження електронного документообігу, використання мережі відеоконференц-зв’язку. У зв'язку з цим виникає необхідність розробки сучасних методів і систем захисту інформації від різних типів загроз у всіх системах.

1. Вирішення проблеми забезпечення безпеки інформації в умовах значного росту її об’ємів, що обробляється інформаційно-телекомунікаційними системами та збільшення ймовірності ризиків, загроз до неї, можливо шляхом розробки сучасних методів та систем захисту інформації.

2. Аналіз можливих методів оцінки можливих загроз для інформації, яка циркулює на об’єкті інформаційної діяльності, свідчить, що жоден із цих методів не може забезпечити повну і адекватну оцінку. Найбільш раціональним

є поєднання декількох методів з урахуванням їх особливостей, тобто — застосування інтегрованого підходу до розробки математичних моделей оцінки загроз з урахуванням декількох методів. При цьому маємо ефект «складання» потужності цих методів та подолання проблем невизначеності вихідної інформації та адекватності розроблених моделей.

3. Серед найбільш прийнятних методів слід виділити наступні: експертні методи (метод безпосередньої оцінки, метод Акоффа-Черчмена); графові методи та відповідні матриці, які відображають причинно-слідчі відносини між всіма елементами (параметрами) оціночної моделі; методи теорії нечітких множин для усунення невизначеності вихідних даних для рішення задач оцінки, формалізації та врахування суб'єктивізму (власних переваг) ОПР; методи теорії ймовірностей, якщо відомі або визначені закони розподілення випадкових величин, що використовуються в оціночної моделі, а також методи теорії прийняття рішень.

4. Розвиток теорії та практики побудови оптимальних (квазіоптимальних) приймачів сигналів та методів цифрової обробки суміші сигналів та завад потребує розроблення та удосконалення методів (засобів) побудови та використання технічних засобів захисту інформації.

5. Одним із важливих напрямків забезпечення процесу створення систем захисту інформації є проведення досліджень методів оцінки якості маскуючих шумів та розробка сучасних норм, методик та рекомендацій щодо побудови та використання технічних засобів захисту інформації.

6. При цьому виникають питання скорочення часу на проведення різних досліджень під час розробки, створення, державної експертизи та оцінки захищеності інформації засобів та систем захисту інформації, що використовуються в інформаційно-телекомунікаційних системах держави.

7. Одним із напрямків підвищення швидкості логічних обчислень є вибір форми представлення, реалізація якої засобами вимірювально-обчислювальної техніки було би найбільш оптимальним.

8. Крім того важливим напрямом в науково-методичному забезпеченні системи інформаційної безпеки є розвиток та удосконалення системи післядипломної освіти. Так Державним університетом телекомунікацій сумісно з представниками організацій-ліцензіатів в галузі технічного захисту інформації та при активній участі фахівців Адміністрації Державної служби спеціального зв'язку та захисту інформації були розроблені та погоджені наступні Програми (таблиця 1).

9. Загальний обсяг часу навчання (тривалість підвищення кваліфікації) за певною програмою визначається навчальним планом і може складати 72, 108, 216 та до 648 годин або від 2 до 18 кредитів (один кредит відповідає 36 годинам). З них розподіл часу між аудиторною, практичною і самостійною роботою здійснюється у майже співвідношенні 1/2/1. Передбачаються аудиторні заняття (лекції, практичні заняття, тестовий контроль знань) та самостійна робота. Може передбачатися проведення практичних занять на базі організацій, установ, яки надають відповідні послуги у галузі технічного захисту інформації.

Таблиця 1.

<table>
<tr><td>«Виявлення закладних пристроїв»</td><td>«Оцінювання захищеності інформації. Атестація комплексів ТЗІ»</td><td>«Оцінювання захищеності інформації. Експертні оцінювання у сфері технічного захисту інформації»</td></tr>
<tr><td colspan="3">Тема 1. Організаційно-правові засади технічного захисту інформації</td></tr>
<tr><td colspan="3">Тема 2. Технічні канали витоку інформації</td></tr>
<tr><td colspan="3">Тема 3. Захист інформації в інформаційно-телекомунікаційних системах</td></tr>
<tr><td colspan="3">Тема 4. Захист інформації, що озвучується на об’єктах інформаційної діяльності</td></tr>
<tr><td>Тема 5. Основні види закладних пристроїв та їх демаскуючи ознаки</td><td rowspan="2">Тема 5. Атестація комплексів ТЗІ</td><td rowspan="2">Тема 5 Державна експертиза в сфері технічного захисту інформації</td></tr>
<tr><td>Тема 6. Способи (методи) та засоби виявлення закладних пристроїв на об’єктах інформаційної діяльності</td></tr>
<tr><td colspan="3">Всього за навчальну дисципліну 72 години</td></tr>
</table>

ЛІТЕРАТУРА:

1. Додонов О.Г., Горбачик О.С., Кузнєцова М.Г. Глобалізація інформаційних систем та безпека // Інформаційні технології та безпека. Зб. наук. праць. — К.: ІПРІ НАН України, 2002. — С.49-53.

2. Довбня С.Я., Кривцун В.І., Четверіков І.О., Савран В.О., Солдатенко О.О. Науково-методичне забезпечення створення та функціонування системи інформаційної безпеки держави. Зб. наук. праць. — К.: ВІКНУ, 2014. — Вип. № 47. — с. 98-108.

В.В. Козловський, д.т.н., проф., Ю.І. Хлапонін, к.т.н., с.н.с.,

А.В. Міщенко, к.т.н, доц., *Національний авіаційний університет*

НЕЧІТКІ НЕЙРОННІ ПРОДУКЦІЙНІ МЕРЕЖІ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

На сьогоднішній день оцінювання рівня захищеності інформації визначається системою кількісних та якісних показників, які забезпечують розв’язання задачі захисту інформації на основі існуючих в державі норм та вимог. За умови стрімких темпів розвитку інформаційних технологій, збільшення кількості загроз інформації, ступеня невизначеності їх виникнення і реалізації, а також складності систем захисту інформації та їх спеціалізованої спрямованості, набуває актуальності завдання отримання узагальненої оцінки

рівня захищеності інформації на основі методології, що враховує як кількісні, так і якісні показники оцінки.

Авторами запропона модель нейромережної системи оцінки рівня захищеності інформації, застосовуючи теорію нечітких продукційних моделей (мереж). Інформація про систему, її параметри, входи, виходи та стан системи може бути не надійною, не чітко визначеною та слабоформалізованою. Модель системи є універсальною, достатньо ефективною, описується мовою, близькою до природньої.

Нечіткі продукційні моделі (Rule-Based Fuzzy Models/Systems) є найбільш загальним видом нечітких моделей, які використовуються для опису, аналізу та моделювання складних, слабоформалізованих систем та процесів. Для оцінки рівня захищеності інформації можуть бути застосовані нечіткі продукційні моделі та алгоритми нечіткого висновку на їх основі.

Формально нечіткі продукційні моделі можуть бути представлені у вигляді нечітких продукційних мереж, які по своїй структурі ідентичні багатошаровим нейронним мережам, елементи кожного шару яких реалізують окремий етап нечіткого висновку в нечіткій продукційній моделі.

Запропоновано створювати нечіткі продукційні моделі системи оцінки рівня захищеності інформації адаптивними (з корекцією в процесі та за результатами їх функціонування), а також реалізовувати різні компоненти цих моделей на основі нейромережевої технології.

УДК 354.42

О.М. Косогов, к. військ. н., с.н.с.,
Міністерство оборони України, olmykos@gmail.com

КОНЦЕПТУАЛЬНІ ОСНОВИ СТВОРЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ОБОРОНИ УКРАЇНИ

Основною метою створення системи забезпечення інформаційної безпеки України у сфері оборони (СІБ СО) є попередження та нейтралізація інформаційних загроз їх функціонуванню; створення умов для сталого та гарантованого виконання Міністерством оборони України та Збройними Силами України завдань, визначених Конституцією та законами України.

З метою визначення елементів системи, їх завдань, доцільно розглянути систему інформаційної безпеки у сфері оборони України як організовану сукупність взаємопов’язаних функціональних підсистем.

1. Підсистеми виявлення інформаційних загроз (виявлення загроз національній безпеці України в інформаційній сфері; виявлення ознак інформаційно-психологічного впливу на особовий склад Збройних Сил України; виявлення джерел, які можуть спричинити виток інформації з обмеженим доступом; виявлення кібернетичних загроз функціонуванню інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем; виявлення невідповідностей стану та можливостей інформаційно-телекомунікаційних систем та інших інформаційних систем військового

призначення сучасним вимогам; виявлення апаратних та програмних закладок на об'єктах інформаційної діяльності Збройних Сил України).

2. Підсистеми аналізу і прогнозування загроз та планування заходів інформаційної безпеки (збір, узагальнення та систематизація даних про інформаційні загрози, їх оцінювання та прогнозування їх розвитку; збір, узагальнення та систематизація даних про факти інформаційно-психологічного впливу на керівництво та населення держави, особовий склад Збройних Сил України; оцінювання джерел інформаційно-психологічного та інформаційно-технічного впливу; визначення об'єктів критичної інфраструктури; планування заходів інформаційної боротьби..

3. Підсистеми протидії інформаційним загрозам (адекватне реагування на кризові ситуації в інформаційному просторі; підготовка та ведення інформаційно-психологічних операцій (заходів);інформаційно-аналітичне забезпечення заходів реагування на кризові ситуації, що спричинюються інформаційними загрозами; комплектування, забезпечення, підготовка та управління застосуванням сил і засобів захисту інформації та кібернетичної безпеки в інформаційно- телекомунікаційних системах).

4. Підсистеми захисту від інформаційних загроз (захист інформаційного простору від кібератак у мирний час та в особливий період; проведення заходів захисту об'єктів критичної інфраструктури; контроль використання інформації з обмеженим доступом; захист особового складу Збройних Сил України від негативного інформаційно-психологічного впливу).

Такий підхід дозволить побудувати раціональну систему інформаційної безпеки у сфері оборони та забезпечити підвищення загальної ефективності протидії загрозам у державному інформаційному просторі.

Список використаних джерел:

1. Ю.І. Радковець, О.В. Левченко, Косогов О.М. Погляди на створення системи інформаційної безпеки України та її Збройних Сил // Наука і оборона. — 2014. — № 1. — С. 38–41.

2. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України : аналітична доповідь / Д.В.Дубов, М.А.Ожеван. — К. : НІСД, 2011. — 30 с

UDC 53.01

E.A. Machusky, prof., D.Sc.

National Technical University of Ukraine "Kyiv Polytechnic Institute",
sivera@ukr.net

MYSTERY OF 137 PRIME OR SIMPLEX QUANTUM THEORY

During the last century the magic number 137 deeply troubles all the scientific community not only physicists.

"...The fact however that alpha has just its value 1/137 is certainly no chance but itself a law of nature. It is clear that explanation of this number must be a central problem of natural philosophy..." (Max Born).

"...You would like to know where this number for a coupling comes from: is it related to pi or perhaps to the base of natural logarithms? Nobody knows. It's one of

greatest dumn mysteries of physics: a magic number that comes to us with no understanding by man...” (Richard Feynman).

The reciprocal number 1/137 is an infinite periodic palindrome decimal fraction:

$$1/137 = 0.007299270072992700729927...$$

Additional remark:

$$(1.11111111111...)^3 = 1.37 + (137 + 1 \cdot 37)/10^5 + (137 + 2 \cdot 37)/10^8 +$$
$$+ (137 + 3 \cdot 37)/10^{11} + +(137 + 4 \cdot 37)/10^{14} + ...$$
$$1/(1.11111111111...)^3 = 0.72900000000...$$

All the fractions $1/(137 \cdot 10^n)$ where $n = ...-4,-3,-2,-1,0,1,2,3,4...$ are the infinite periodic decimal palindromes.

Reciprocal 1/137 is simply the coupling number of the positional calculation systems!

Now we can introduce the Quantum Calculation System using the natural calculation system, basic physical constants and equations of Newton, Kelvin, Avogadro, Boltzmann, Faraday, Maxwell, Planck, Einstein, Zommerfeld, Heisenberg, Shredinger, Josephson, von Klitzing and many others. Let us:

$$\text{Universal diameter } D_U = e \approx 2.718281828459045...,$$

$$\text{Universal perimeter } P_U = \pi \cdot e \approx 8.539734222643...,$$

$$\alpha_0 = (\pi \cdot e/100)^2 \approx 0.00729270505939...,$$

$$\alpha_1 = 1/137 \approx 0.007299270072992700729927...,$$

$$\text{Finite difference } FD = (\alpha_1 - \alpha_0) \approx 0.0000065640136...,$$

$$\text{Finite ratio } FR = \alpha_1 / \alpha_0 \approx 1.00090007927...,$$

$$\alpha_n = \alpha_0 + n \cdot FD, n = ...-4,-3,-2,-1,0,+1,+2,+3,+4... .$$

Planck numbers are expressed by author as the stepped circle perimeters of Euler spiral:

$$h_n = 2 \cdot \pi \cdot (1 + 2 \cdot (e + \alpha_n \cdot (1 + \sqrt{2 \cdot \pi \cdot e/100}))/100)$$

Planck constant is $h_n(\alpha_0)$:

$$h_0 = 2 \cdot \pi \cdot (1 + 2 \cdot (e + \alpha_0 \cdot (1 + \sqrt{2 \cdot \pi \cdot e/100}))/100) \approx 6.62606983982...$$

(current CODATA value is 6.62606957(29) and proposed conventional value is 6.62606X....).

Boltzmann constant is expressed by author as time-delay angle difference of harmonic oscillator Wien shifting:

$$k = \cos(12 - \alpha_0/10) - \sin(12 - \alpha_0/10) \approx 1.38065060066...$$

(current CODATA value is 1.3806488(13) but proposed temperature balancing value is 1.38065X).

Avogadro constant is expressed by author as the median information entropy number:

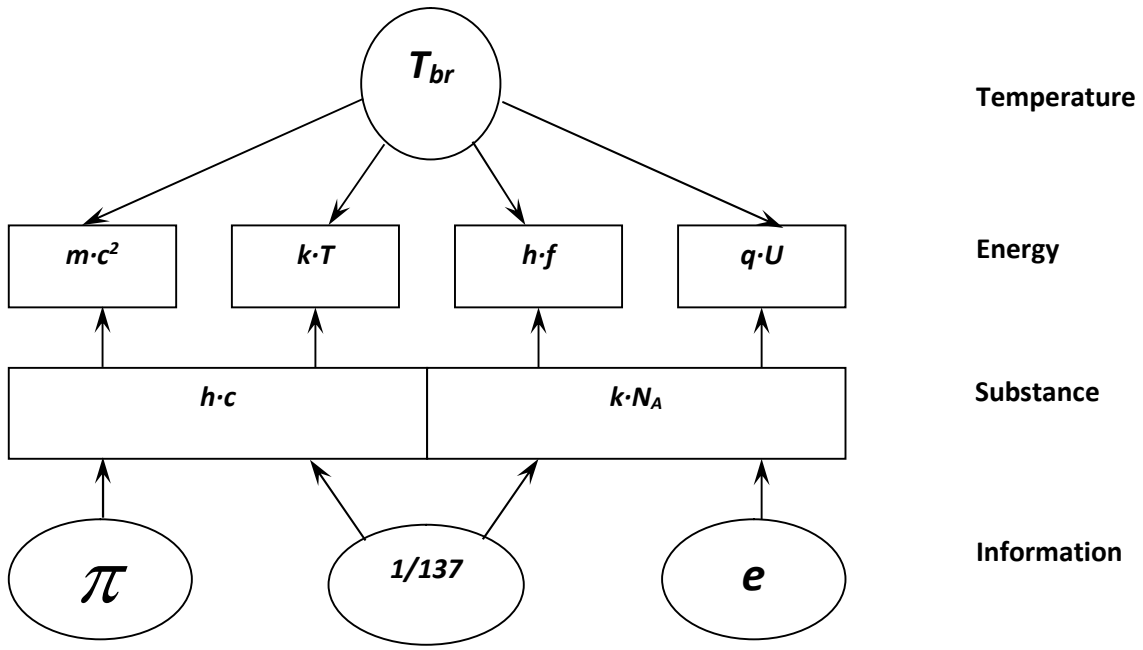
$$N_A = [2 \cdot \sqrt{2 \cdot \pi \cdot e} / \sqrt{8 \cdot \pi \cdot e + 137^2} / (1 + 2 \cdot \alpha_0 / 1000)]_{-1/10000}^{+0} \cdot 100 =$$
$$= 6.02214128 \pm 50 \cdot 10^{-7}$$

(current CODATA value is 6.02214129(27) and proposed 6.02214X...).

Decimal order of constants depends upon measuring system units of length, time, mass. Than mass *m* is a volume density of gravitation field and electric charge *q* is a surface density of the gravitation field. The basic energy sources of universe are the microwave background radiation $T_{mbr} = e + \alpha \pm N_A / 1000$ and the macrowave substance background radiation $T_{sbr} = e - \alpha \pm N_A / 1000$, where $N_A / 1000$ is corresponding temperature anisotropy caused by Newtonian gravitation constant *G* dispersion.

$$G_0 = h_0 \cdot (1 + \alpha_0 + 5 / x) / 2 \approx 6.67352418955...,$$

where *x* is the root of the black body radiation equation exponential parameter, $x \approx 4.96511423174...$



And one more remark: mysterious fine structure constant:

$$FSC = 1 / \sqrt{\pi^2 + 137^2} \approx 0.00729735168... \quad (8)$$

All the rest fundamental constants we can calculate using listed above with an accuracy restricted only by the decimal order of pi and e. Limiting factor is $\alpha \cdot 10^{-57}$.

УДК 004.056.5

О.Г. Оксіюк, О.І. Кохановський

Київський національний університет імені Тараса Шевченка

ВИРІШЕННЯ ПИТАНЬ ЩОДО ПІДГОТОВКИ/ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ФАХІВЦІВ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. СУЧАСНИЙ ПІДХІД

Сучасний світ ставить завдання щодо забезпечення швидкої та якісної підготовки фахівців у галузі ІБ. Надзвичайно важливо — можливість практичного підготовки слухачів з питань безпосереднього вирішення питань забезпечення безпеки у інформаційних системах.

Це призводить до необхідності радикальної зміни підходів до учбового процесу, а саме:

- проведення наукових та дослідно-пошукових робіт, спрямованих на опрацювання наукових питань побудови захищених систем та забезпечення можливості математичного обґрунтування захищеності;
- створення наукових та навчальних лабораторій, які виступають в якості полігонів для опрацювання питань вивчення слухачами сучасних технологій та обладнання для побудови захищених систем;
- залучення фахівців провідних установ та організацій для практичного проведення робіт в межах наукових лабораторій.

Кафедрою інформаційної безпеки ФІТ спільно з фахівцями комерційних організації вже опрацьовуються питання щодо спільного створення такої лабораторії, проведення наукових досліджень.

На наш погляд першочерговими є наступні науково-технічні завдання:

Побудова математичної моделі оцінки захищеності складних розподілених інформаційно-телекомунікаційних систем.

Складність даної задачі полягає в тому, що корпоративні інформаційні системи на поточний час суттєво зросли, важливість інформації, що обробляється, накопичується, зберігається в таких системах на багато перевищує вартість самих систем. Ризики щодо втрати інформації, блокування доступу до інформації, можливості нав’язування хибної інформації надзвичайно зросли.

На наш погляд для забезпечення безпеки інформації, обґрунтованого вибору напрямів розвитку систем забезпечення ІБ в ІТС повинні використовуватись математичні методи оцінки інформації.

Побудова ймовірносної та статистичної моделі оцінки захищеності складних інформаційних систем.

На поточний час існує велика кількість інформаційних систем, які потребують подальшої модифікації та розвитку систем захисту інформації. В той же час в сучасних економічних умовах питання обґрунтування вибору першочергових заходів, які потребують фінансових або ресурсних вкладень, є надзвичайно актуальним.

Вважаємо, що використання математичних ймовірностних методів, методів теорії можливостей, статистичних методів надасть можливість здійснять обґрунтування та математичне доведення напрямів розвитку систем захисту інформації в корпоративних системах.

УДК 004.932.4

Д.А. Прогонов, П.П. Яцура, С.Н. Кущ
Физико-технический институт, Национальный технический университет Украины «Киевский политехнический институт»
progonov@gmail.com

ДЕСТРУКЦИЯ СТЕГАНОГРАММ С ДАННЫМИ, ВСТРОЕННЫМИ В ОБЛАСТИ ПРЕОБРАЗОВАНИЯ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ

Широкое распространение сервисов обмена цифровыми изображениями (ЦИ), а также наличие в свободном доступе значительного количества стеганографических программ для скрытия сообщений в области преобразования цифровых изображений (ОПЦИ), существенно упрощает создание робастных каналов обмена данными между злоумышленниками. Применение современных методов пассивного стегоанализа ЦИ для распознавания наличия стегоданных не всегда является возможным, вследствие их высокой вычислительной сложности [1], а применение более простых алгоритмов приводит к снижению точности обнаружения стеганограмм. Поэтому при обработке передаваемых изображений в качестве превентивной меры могут использоваться методы активного стегоанализа (АС). Особый интерес представляет применение стандартных методов обработки (СМО) ЦИ для деструкции стегоданных, встроенных в ОПЦИ, учитывая высокую эффективность данных методов при проведении АС стеганограмм, сформированных классическими LSB-методами [2].

В работе исследована эффективность применения СМО изображений, а именно медианной фильтрации (МФ), для разрушения стеганограмм, сформированных в ОПЦИ с применением двумерного дискретного вейвлет преобразования (ДДВП) [3]. В качестве базисной функции ДДВП были использованы вейвлет Хаара и, соответствующая ему, скейлинг-функция. Степень заполнения изображения-контейнера (ИК) стегоданными (отношение модифицированных коэффициентов ДДВП к общему количеству коэффициентов разложения ИК) варьировалась от 5% до 25% с шагом 5% и от 25% до 95% с шагом 10%. Размер МФ при проведении обработки стеганограмм изменялся от 5×5 (пикселей) до 23×23 (пикселей) с шагом 6 (пикселей). Для оценки искажений ИК и стегоданных при проведении МФ были использованы 6 стандартных метрик качества (МК) ЦИ — Mean-Squared Error (MSE), Image Fidelity (IF), Normalized Cross-Correlation (NCC), Czenakowski Distance (CD), Peak Signal-to-Noise Ratio (PSNR), Structure Similarity (SSIM).

По результатам анализа полученных данных установлено, что степень заполнения контейнера, при которой искажения стегоданных и ИК являются минимальными, равна 10% (размер МФ 5×5 (пикселей)) и увеличивается при

возрастании размера МФ. Повышение степени заполнения ИК приводит к возрастанию искажений встроенных сообщений при сохранении фиксированного уровня изменений ИК, что позволяет скрывать факт проведения атаки на стеганограмму. Выявленная тенденция сохраняется для всех рассмотренных МК.

Полученные результаты могут быть использованы для повышения эффективности существующих методов АС, а также маскирования факта проведения атаки на стегосистему.

Список литературы:

1. Holub V. Random Projections of Residuals for Digital Image Steganalysis / Holub V., Fridrich J. // IEEE Transactions on Information Forensics and Security. — 2013. — Vol. 8, Issue 12. — p. 1996-2006.

2. Черепахова К.В. Медіанна та двовимірна вінеровська фільтрація стеганограм / Черепахова К.В., Прогонов Д.О., Кущ С.М. — Матеріали XII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». — К.: ВПІ ВПК «Політехніка», 2014. — с. 222-224.

3. Dey N. A novel approach of color image hiding using RGB color planes and DWT / Dey N., Roy A.B., Dey S. // International journal of computer application. — Vol. 36, No.5 — 2011. — p.19-24.

УДК 681.61

Ю.Я. Самохвалов

Київський національний університет імені Тараса Шевченка

О.И. Бурба

Державний інститут науково-технічної та інноваційної експертизи

ПЛАНИРОВАНИЕ МЕРОПРИЯТИЙ ПО МИНИМИЗАЦИИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В последние годы многие компании и организации всех форм собственности хорошо осознали необходимость управления информационной безопасностью предприятия. Чтобы надежно защитить важнейшую деловую информацию, компаниям необходимо интегрировать вопросы физической и информационной безопасности в единый для всей организации процесс — процесс управления информационной безопасностью предприятия**.**

Основными функциями систем управления информационной безопасностью являются: выявление и анализ рисков информационной безопасности: планирование и практическая реализация процессов, направленных на минимизацию рисков: контролирование этих процессов и внесение в процессы минимизации информационных рисков необходимых корректировок.

В настоящее время для реализации этапов выявления и анализа рисков информационной безопасности, а также контроля этих процессов используются известные стандарты и соответствующие апробированные методики. Вместе с тем методическому обеспечению планированию мероприятий по минимизации

рисков, в настоящее время незаслужено мало уделяется внимание. В докладе рассматривается один из возможных подходов к планированию мероприятий, в основу которого положено совместное использование усовершенствованного метода прогнозного графа В.М.Глушкова [1] и метода анализа иерархий Т. Саати [2].

Использование усовершенствованного метода В.М.Глушкова позволяет сформировать прогнозного графа мероприятий по минимизации рисков, а методом анализа иерархий в этом графе выбирается наиболее рациональный план, характеризующийся временем его реализации и необходимыми для этого ресурсами.

Литература

1. Самохвалов Ю.Я.,Науменко Е.М., Бурба О.И. Использование нечетких оценок в методе прогнозного графа/ Реєстрація, берігання і обробка даних. — 2010. — Т.12, № 4. — С. 22-30

2. Саати Т. Принятие решений. Метод анализа иерархий. — М.: Радио и связь, 1993. — 311 с.

УДК 004.056:061.68

Синицын И.П., д.т.н., Колтик М.А.

Институт програмних систем НАН Украины, г.Киев, Украина

АНАЛИЗ ПОСТРОЕНИЯ МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ОНТОЛОГИИ СОЗДАНИЯ И ПРОВЕДЕНИЯ ИСПЫТАНИЙ КСЗИ

В общих чертах под онтологией понимается система понятий некоторой предметной области, объединенных некоторой общей концептуальной сущностью и соединенных различными отношениями. Онтологии используются для формальной спецификации понятий и отношений, которые характеризуют определенную область знаний. Преимуществом онтологий в качестве способа представления знаний является их формальная структура, которая упрощает их компьютерную обработку [1].

Анализ технологии создания и проведения испытаний КСЗИ позволяет говорить о возможности и целесообразности использования системно–онтологического подхода для рассмотрения данной предметной области и, в частности, построения модели угроз и нарушителей информации. Данный подход подразумевает создание онтологии, которая рассматривается как составной компонент (база знаний) средства автоматизированной поддержки создания и проведения испытаний КСЗИ [2].

Возможность использования онтологии в качестве узкоспециализированной базы знаний, из которой пользователь может извлечь необходимые для него знания, при построении модели угроз и нарушителей информации является актуальной практической задачей.

В общем случае **методика проектирования онтологии** включает три этапа:

1. Предварительный анализ заданной предметной области;

2. Построение онтологического графа предметной области. Под онтологическим графом понимается ориентированный граф, вершинами которого являются понятия предметной области, а дугами — связи, отношения между ними.

3. Графическое (визуальное) проектирование онтологического графа предметной области и составление формализованного описания онтологии предметной области [2].

Центральной идеей используемой при проектировании онтологии является модульный подход. Каждый из выделенных модулей, отвечает за выполнение отдельных функциональных задач и решение отдельных вопросов. Каждый модуль выделяется исходя из специфики рассматриваемой предметной области и выполняемых им задач на определенном этапе технологического процесса. [3]

Для построения модели угроз и модели нарушителей информации выделяются следующие онтологические модули: «Модель угроз», «Модель нарушителя». Они на концептуальном уровне, описывают (моделируют) онтологическую систему процесса построения модели угроз и нарушителей информации.

Графическое (визуальное) представление модуля «Модель угроз» представлено на Рисунке 1 и Рисунке 2. Полное их описание представлено в статье [3].

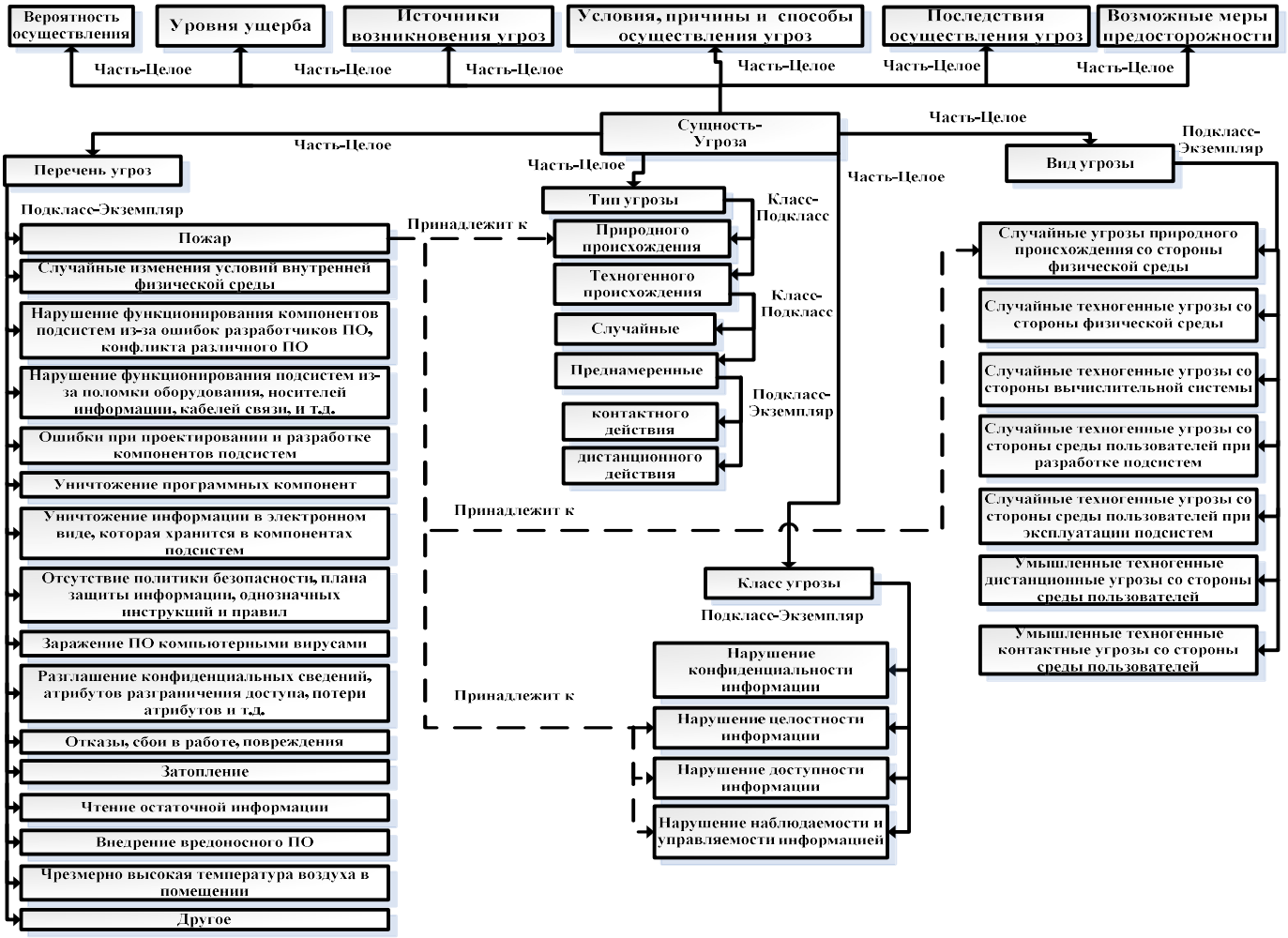


Рисунок1 — Модуль «Модель угроз» (1)

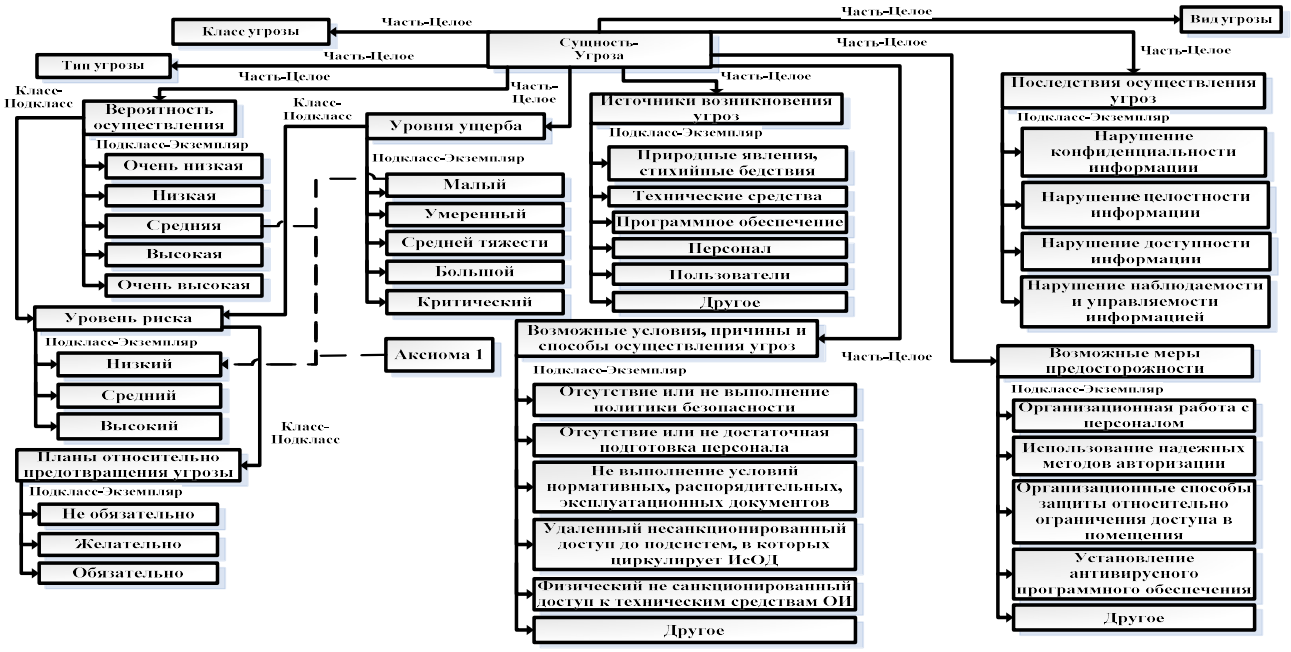


Рисунок 2 — Модуль «Модель угроз» (2)

Графическое (визуальное) представление модуля «Модель нарушителя» представлено на Рисунке 3. Полное его описание представлено в статье [3].

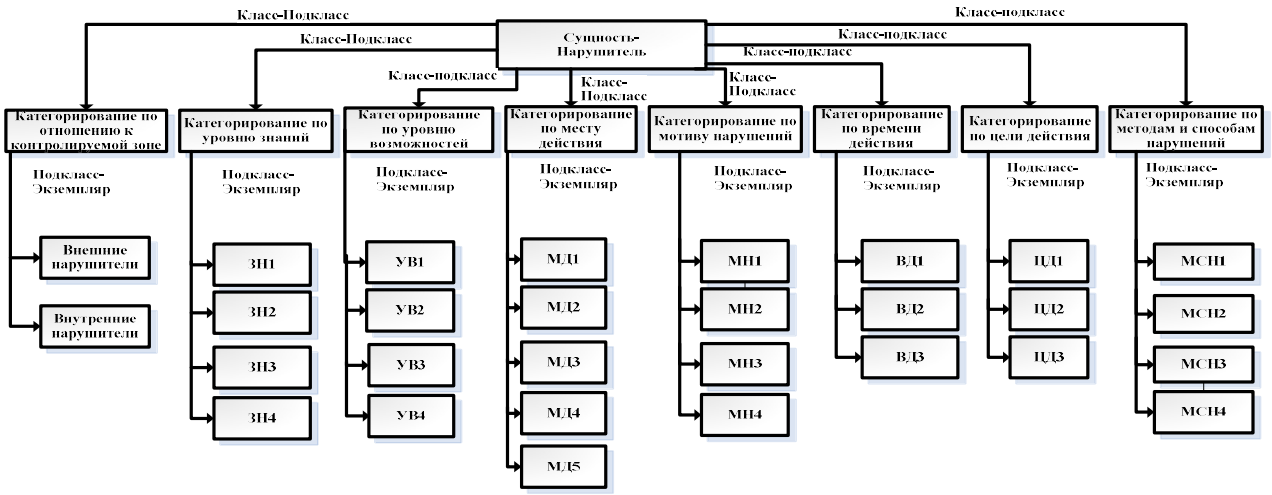


Рисунок 3- Модуль «Модель нарушителя»

Подробное описание представленных модулей и их взаимодействия представлено в статье [3].

Каждый модуль содержит: **понятие — сущность** (исходное понятие, которое является вершиной для построения графа понятий выделяемого онтологического модуля), **понятия** (множество объектов, которые принадлежат к некой общей сущности рассматриваемой предметной области, связаны между собой отношениями и могут быть упорядочены иерархически, **классы (подклассы) понятий** (группа индивидуальных сущностей (понятий), которые объединены на основании наличия общих свойств), **отношения** (связывают между собой понятия (классы, подклассы, экземпляры понятий) и описывают их), **аксиомы** (задают условия соотнесения понятий и отношений, они выражают очевидные утверждения, связывающие понятия и отношения).

Построение представленных онтологических модулей является необходимым условием при разработке онтологии создания и проведения испытаний КСЗИ использование которой, в качестве базы знаний, позволяет

осуществить интеллектуально-информационную поддержку пользователя (разработчика, эксперта) в данной предметной области.

Література

1.Н.С. Константинова, О.А. Митрофанова «Онтологии, как системы хранения знаний». http://window.edu.ru/resource/795/58795/files/68352e2-st08.pdf.

2. М.А. Колтик «Системно-онтологический анализ предметной области проведения испытаний КСЗИ». «Проблемы программирования» «ИПС» НАН Украины № 1 2014 год.

3. М.А. Колтик «Характеристика особенностей построения модели угроз и нарушителей информации для объекта испытаний с использованием онтологии проведения испытаний КСЗИ» «ИПС» НАН Украины № 1 2015 год.

УДК 004.056.5

О.В. Соснін

завідувач кафедри «Міжнародна інформація» Інституту міжнародних відносин Національного авіаційного Університету, доктор політичних наук, професор, заслужений діяч науки і техніки України, член-кореспондент Української академії політичних наук

ПРО ПОТРЕБУ ІННОВАЦІЙНОГО ОНОВЛЕННЯ СЕНСУ ПРОБЛЕМ БЕЗПЕКИ

Людство протягом століть вирішувало світоглядні питання щодо істинної цінності наукових знань і інформації як певної нематеріальної субстанції, а аналіз її різноманітних властивостей і характеристик лише із середини XX ст. став першопричиною зародження і бурхливого розвитку незнаних до цього наукових дисциплін, як то: документалістика (наука про оптимальне управління документованими інформаційними системами), кібернетика (наука про оптимальне управління великими динамічними системами), інформатика (наука про властивості інформації і методи її опрацювання сучасними засобами зв’язку), інформаційне право (наука про правове регулювання інформаційної діяльності) та інші. Протягом останніх десятиліть вони, з одного боку, сформували матеріальне середовище життя сучасної людини, виступили як джерело інноваційних процесів для промислових, наукових, освітніх і управлінських технологій, а з іншого — явили собою основний засіб для встановлення міжособистісних взаємовідносин — комунікації. Поглинаючи весь попередній досвід створення архітектури світових систем управління — від колоніальних імперій європейських країн до глобальних світових корпорацій, побудованих США в XX ст., вона вибудовує новий світ на засадах точного аналізу і коректності в поведінці із змістовною інформацією. (Остання є невіддільною від якості комунікації, тобто, виступає як певний атрибут комунікації.)

Володіючи фундаментальною властивістю — цінністю, змістовна інформація, як і комунікація, завжди є аксіогенною. Як наслідок, всяка інформаційно-комунікаційна робота є аксіогенною і одночасно й культурогенною, а тому завжди потребує обмежень і захисту з боку держави.

Робота із інформацією в умовах впровадження новітніх інформаційно-комунікаційних технологій (ІКТ) створює нові інформаційно-технологічні реалії з точки зору обмежень і безпеки у всіх сферах людської діяльності. Нові для людини, суспільства і держави проблеми безпеки відкривають величезні предметні простори і об'єкти досліджень, зокрема і щодо інформаційної природи нових викликів й загроз. Сучасна небезпека зазвичай має високотехнологічний і складний зміст, а тому одним із найактуальніших завдань науки і освіти про безпеку людини, суспільства, держави наразі стає мобілізація всіх теоретичних, методологічних і практичних знань, накопичених людством, для організації досліджень, спрямованих на усвідомлення і попередження загроз. Особливо для інформаційно-комунікаційних феноменів, які виникають при комп'ютерному опрацюванні інформації в засобах зв'язку.

Сьогодні, спостерігаючи життя і процеси інноваційного оновлення світу науки, освіти, промисловості, боротьбу політичних партій і їх лідерів за владу, аналізуючи події, які відбуваються в Україні, ми дедалі більше усвідомлюємо могутність факторів впливу на інформаційно-комунікаційні чинники і значимість процедур захисту інформації. Ми бачимо, що без їх глибокого усвідомлення реальні загрози для інформації і комунікації постійно будуть зростати, а тому надалі неможливо уявити наше загальне інноваційне оновлення без впровадження ідеології захисту до всіх процедур обміну інформацією та знаннями.

Аналізуючи темпи оновлення інформаційно-комунікаційної інфраструктури, ми бачимо, що в світі, який нас оточує, постійно зростають безпекові вимоги, коли йдеться про формування нових форм управління людиною, суспільством, державою. Ми бачимо, що новий клас управлінців (нетократія (англ. *netocracy*), інфократія (англ. *infocracy*), медіократія (англ. *mediocracy*)), який переводить нас і нашу свідомість в іншу — віртуальну реальність, активно її використовує тому, що в штучно сконструйованому кібернетичному просторі існує мінімальна кількість перешкод для поширення інформації.

За таких умов виключно актуальними стають розробка національних концепцій і стратегій розвитку освіти в Україні на 2012-2021 роки та різних науково-освітніх концепцій і класифікацій. Підготовка фахівців з проблем захисту інформації і вивчення проблем безпеки інформаційного обміну для потреб інноваційного розвитку країни, на наш погляд, стала ключовим фактором при проведенні всіх інших реформ в державі. Скажімо, що під впливом Інтернет людське суспільство дедалі більше стає «електронним класовим суспільством», в якому, крім комфорту спілкування, зростає напруженість, несправедливість і нерівність, що прирікає людство на ескалацію соціальних конфліктів і спонукає до бунтарства і громадянських війн.

Міжнародна практика свідчить, що розвиток ІКТ в останні роки всюди сприяв підвищенню вагомості інформаційно-комунікаційної функції держави, розширив сферу відповідальності владних структур за можливість негативного інформаційного впливу на суспільство, як «м'якої» («розумної») сили, так і «жорсткої» (летальної) зброї сучасних інформаційних війн, і, як наслідок, підвищив рейтинг проблем безпеки. Ми бачимо, що новітні ІКТ стрімко і впевнено диференціюють і інтегрують в собі (в залежності від вимог) будь-яку

сферу людської діяльності. Постійно розширюючи свої можливості, вони входять навіть у такі традиційно закриті для широкого загалу сфери, як то дипломатія і споріднені із нею галузі, які завжди використовували утаємничені методи комунікації. В світі сьогодні стрімко вибудовуються засади цифрової (Digital Diplomacy) або мережевої (Net Diplomacy) дипломатії. (Означається також терміном «публічна дипломатія Веб 2.0» — Public Diplomacy Web 2.0.) З ініціативи світових лідерів — США й Великобританії, в 2011 році засноване міждержавне партнерство «Відкрите урядування» (Open Government Partnership, OGP), до якого у даний момент входять 64 держави, які взяли на себе зобов'язання розкрити інформацію про діяльність національних урядів і радикально змінити систему управління суспільством і міжнародні інформаційно-комунікаційні відносини.

Таким чином, на відміну від попередніх періодів, проблема контролю безпеки комунікації, особливо, транснаціональної, набуває в житті людини, суспільства і держави особливого значення. Як наслідок, зростає потреба в якісно нових методів підготовки фахівців, зокрема і для здійснення нових підходів в організації інформаційно-комунікаційної політики держави. Сьогодні ми бачимо, що Україна, начебто, і набула незалежності, і має ознаки державності, але не змогла поки що побудувати державу, яка управляє своїм інформаційно-комунікаційним середовищем, — стала просто територією (полігоном) для величезних інформаційно-комунікаційних і фінансово-економічних маніпуляцій із своїм народом. За відсутності залучених до здійснення інформаційно-комунікаційної політики інтелектуалів, ми широко розплющеними очами дивимось як падає, руйнуючись, все, що вважали для себе вічним, і як зростає рівень протистояння людей і їх суспільно-політичних об’єднань. Нас дедалі більше поглинає глобальна (за виміром) інформаційно-комунікаційна війна і ми втрачаємо вплив на процеси міжнародного суперництва країн за володінням абсолютним ресурсом розвитку — інформацією і ринками освіти. Тут для нас вже багато що втрачено і виникла значна нерівність, подолати яку буде виключно важко.

Все це, безумовно, ускладнює загальну безпекову ситуацію в країні, оскільки розширюється коло обізнаних в проблемах безпеки фахівців — прибічників і опозиційно налаштованих до дій влади, що вимагає від держави певних зусиль при організації їх інформаційно-комунікаційної взаємодії.

За таких умов саме життя вимагає від нас інноваційно оновити наукові і освітні програми підготовки фахівців для інформаційно-комунікаційної діяльності, як специфічної складової при викладанні всіх наук. Перш за все, потрібно органічно, по новому і якісно, поєднати викладання технічних і гуманітарних дисциплін. Крім теоретичних знань, від викладачів тут потрібний практичний досвід роботи і здатність до інформаційно-пропагандистського забарвлення навчального процесу, оскільки майбутнім фахівцям потрібно, крім знань про сутність і організацію інформаційно-комунікаційної роботи, дати чіткі уявлення про глобальне інформаційно-комунікаційне протистояння, яке виникло у світі.

І.Ю.Субач д.т.н, О.Я Васильєв
Військовий інститут телекомунікацій та інформатизації
Державного університету телекомунікацій

ВІЗУАЛІЗАЦІЯ ДАНИХ У СИСТЕМІ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ АТАК

Одним із важливих засобів захисту від кібернетичних атак є системи виявлення атак (СВА) — програмні або апаратні засоби, які призначені для виявлення фактів неавторизованого доступу у комп'ютерну систему або мережу або несанкціонованого керування ними. Проте, незважаючи на той факт, що у теперішній час питанням побудови СВА присвячено велику кількість наукових робіт, головне питання — ефективне застосування СВА для побудови системи кібернетичного захисту, залишається не вирішеним.

Це обумовлює актуальність подальших досліджень, які полягають у підвищенні ефективності застосування СВА на основі розробки та впровадження нових методів виявлення кібернетичних атак.

Аналіз останніх досліджень і публікацій показує, що методи виявлення атак у сучасних СВА недостатньо повно опрацьовані з точки зору стійкості, адаптованості та верифікації, а також достатньо складно оцінити їхні властивості такі, як обчислювальна складність, коректність, завершуємість та інші.

Найбільш ефективною можна вважати СВА, яка: є повною (покриває всі класи атак); дозволяє аналізувати поведінку інформаційної системи (ІС), яка захищається, на всіх рівнях (мережевому, вузловому, окремих додатків тощо); є адаптивною до всіх типів атак; масштабується для різних класів ІС (від локальних до корпоративних); є відкритою; має вбудовані механізми реагування на атаки; є захищеною від атак на свої компоненти.

На сьогоднішній день, жодна з СВА у повній мірі не відповідає сформульованим критеріям, зокрема завдяки відсутньої адаптації до невідомих типів атак та неможливості аналізувати поведінку ІС на всіх рівнях одночасно.

Для усунення даних недоліків, є доцільним проведення низки наукових досліджень щодо розробки адаптивної СВА, в основу функціонування якої необхідно покласти методи, які б при низькій (близькій до лінійної) обчислювальній складності, стійкості та верифікації мали б низькій рівень хибних спрацьовувань.

Результати дослідження сучасних СВА з відкритим кодом (*Snort, Bro, OSSEC, Prelude*) показують, що основними елементами, які входять до їхньої структури є: підсистема збору інформації, що використовується для збору первинної інформації про систему, яка захищається; підсистема аналізу (виявлення), що здійснює пошук атак та вторгнень у систему, яка захищається; підсистема візуального представлення даних (користувацький інтерфейс), який дозволяє адміністратору безпеки спостерігати за станом системи.

Підсистема візуального аналізу даних повинна виконувати функції пошуку прихованих закономірностей у даних, що накопичуються системою, шляхом збігу можливостей сучасних засобів обчислювальної техніки з творчим та гнучким мисленням людини. Це досягається завдяки представленню великих об'ємів даних у формі, яка дозволяє людині побачити те, що важко виділити алгоритмічним шляхом. Візуальний аналіз даних є корисним тоді, коли мало що відомо про самі дані, а цілі дослідження є нечіткими.

У цьому випадку, адміністратор безпеки системи безпосередньо працює з даними, що представляються у вигляді візуальних образів та які він може розглядати з різних сторін, під будь-якими кутами та має можливість отримувати додаткову інформацію, яка допомагає йому більш чітко формулювати цілі аналізу.

Лише часткова практична реалізація запропонованих у доповіді рішень на базі СВА *Bro, OSSEC* та *Prelude*, дозволяють зробити висновок про підвищення ефективності роботи адміністратора безпеки щодо прийняття ним оперативних й обґрунтованих рішень на виявлення та протидію кібернетичним атакам не менш ніж на 15-18%.

УДК 621.287.2

С.В. Толюпа, В.А. Дружинін
Державний університет телекомунікацій

ЗАСТОСУВАННЯ ТЕОРІЇ ДЕКОМПОЗИЦІЇ ДЛЯ ОЦІНКИ ЕФЕКТИВНОСТІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Проблема багатьох інфокомунікаційних систем (ІКС) зв'язку зводиться до того, що кількість параметрів, необхідних для опису поводження системи (розмірність системи), виявляється дуже великою і прийняти правильне рішення в таких мережах досить складно, враховуючи, що інформація про стан мережі може бути досить суперечливою. Збільшення розмірності сучасної технології представляється об'єктивною тенденцією, яку можна спостерігати в історичному зрізі протягом усього розвитку цифрових ІКС.

Гарантування безпеки інформації в мережах нового покоління взагалі та їх системах управління є складним комплексним завданням. У міжнародних стандартах проблеми захисту інформації вирішуються одночасно зі стратегічними та конкретними питаннями розвитку архітектури мережі. Такий підхід відповідає комплексному характеру забезпечення безпеки інформаційних систем на всіх етапах їх життєвого циклу — від концептуальних схем та проектування до технічної експлуатації та використання. Окремими заходами досягти мети, як правило, не вдається й тому в кожному випадку потрібно розглядати всю систему в комплексі, причому захищеність усієї інфокомунікаційної системи (мережі) визначається рівнем захищеності її найбільш слабкої частини.

Бурхливий розвиток інфокомунікаційних систем у напрямку збільшення їх розміру та ускладнення, розширення спектру послуг, які надаються

абонентам, росту кількості компаній, які займаються проектуванням, експлуатацією пов'язаних між собою мереж, що належать різним власникам, необхідність підвищення надійності роботи мережі, якості обслуговування, економічної ефективності та інших вимог, провідні фірми та корпорації світу прийшли до однозначного висновку — необхідності створення гнучкої та надійної системи управління й ними, що і дасть можливість повисити якість ефективності функціонування системи в цілому.

Внаслідок критичних ситуацій, які виникають в мережах, та неспроможності відвернути їх, почались пошуки нових принципів, методів та засобів управління ефективністю системи. Одним з варіантів вирішення цієї проблеми є застосування штучного інтелекту.

Від вибору критерію й системи показників якості (СПЯ) багато в чому залежить результат оцінки і його практична цінність. Загальноприйнятим підходом до розробки системи показників якості складних систем є формулювання безлічі локальних СПЯ, що відповідає сукупності властивостей ІКС, які впливають на виконання поставлених перед нею завдань. Глобальна СПЯ, що характеризує загальну, єдину задачу, яка стоїть перед інфокомунікаційною системою, реалізується шляхом з'єднання вихідних локальних систем показників якості.

Пропонується метод формування системи показників якості, відмінний від традиційного, тобто пропонується, ґрунтуючись на математичних методах теорії декомпозиції (факторизації, функціональної й параметричної декомпозиції), замість визначення локальних СПЯ (ЛСПЯ) низького рівня ієрархії й наступного їхнього об'єднання в глобальну СПЯ (ГСПК) розглядати завдання функціонування ІКС у цілому. При такому підході до оцінки ефективності інфокомунікаційної системи зростає розмірність завдання, яке розв'язується, оскільки формулюється не одна ГСПЯ, а сукупність ієрархічно зв'язаних ЛСПЯ, але зате забезпечується конструктивність рішення завдання й ураховуються реальні поточні ймовірнісні характеристики приватних показників ефективності (ППЕ). Повнота такої СПЯ ґрунтується на тім, що вихідними даними для її формулювання є вимоги, які запропоновані користувачем до ІКС, математично коректно декомпозовані в інтересах їхнього подальшого використання.

УДК 621.396.2

Шевченко А. С.

Військовий інститут телекомунікацій та інформатизації, assheva@gmail.com

ОЦІНКА БЕЗПЕКИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ВІЙСЬКОВИХ СИСТЕМ РАДІОЗВ'ЯЗКУ НА ЕТАПІ ПРОЕКТУВАННЯ З УРАХУВАННЯМ ФУНКЦІОНУВАННЯ В УМОВАХ ВПЛИВУ ІНФОРМАЦІЙНИХ АТАК

Аналіз бойових дій на сході України, показує, що більш чітко проглядається тенденція зростання ролі інформаційних операцій під час воєнних дій, основним видом яких є інформаційні атаки.

Під час конфлікту значна кількість інформаційних атак направлена на порушення захищеності інформації, що передається через інформаційну інфраструктуру інформаційно-телекомунікаційних систем (ІТС) спеціального призначення. На сьогоднішній час, при веденні бойових дій, основним видом зв'язку є радіозв'язок, який є найбільш вразливою частиною ІТС під час інформаційного конфлікту.

На сьогоднішній час у Збройних Силах України заходи з забезпечення безпеки зв'язку не передбачають оцінки інформаційної безпеки (ІБ) військових систем радіозв'язку (СРЗ) для умов впливу інформаційних атак, що відповідно не дає змоги визначити ризики ІБ критичних елементів інформаційної інфраструктури СРЗ. Загрози інформаційних атак розглядаються окремо та не в повному обсязі. З огляду на це, актуальним є розробка методів оцінки ІБ інформаційної інфраструктури систем радіозв'язку спеціального призначення в умовах впливу інформаційних атак.

Зважаючи на проблематику оцінки ІБ, **метою роботи** є підвищення захищеності військових СРЗ в умовах впливу навмисних інформаційних атак на фізичному і канальному рівнях.

Для досягнення поставленої мети, необхідно здійснювати вибір ефективних механізмів захисту інформації (МЗІ) під час проектування військових СРЗ. Для визначення міри ефективності МЗІ пропонується використовувати рівень ризику інформаційної безпеки, що існує при його застосуванні.

Відповідно до цього, в розрізі досягнення мети досліджень, **завданням роботи** є розробка науково-методичного апарату для оцінки безпеки інформаційної інфраструктури військових СРЗ на етапі проектування з урахуванням функціонування в умовах впливу інформаційних атак.

Відповідно до серії міжнародних стандартів ISO 2700x, державної нормативно-правової бази з інформаційної безпеки та захисту інформації, управління ІБ представляє замкнений процес який супроводжує весь життєвий цикл функціонування систем захисту інформації. До основних складових етапів управління ІБ відносяться: аналіз умов функціонування системи, визначення вразливостей та загроз, оцінка порушника та збитків внаслідок атак, безпосередньо оцінка ІБ на основі оцінки ризиків.

Модель управління інформаційною безпекою СРЗ представляє собою замкнену структуру (рис. 1). Відповідно до міжнародних підходів ключовим елементом управління інформаційною безпекою є оцінка ризиків.

На моделі інформаційної безпеки СРЗ (рис. 1) $A = (a_1, a_2, \dots a_\sigma \dots a_\Omega)$ — множина типів атак; $S = (s_1, s_2, s_3 \dots s_8)$ — множина типів загроз військовим СРЗ; $Pr = (\rho_1, \rho_2, \dots \rho_\chi \dots \rho_X)$ — множина типів порушників інформаційної безпеки військових СРЗ; $Vr = (\nu_1, \nu_2, \dots \nu_\chi \dots \nu_X)$ — множина типів вразливостей військових СРЗ; $Q = (D_1, V, C, \Delta t)$ — множина параметрів СРЗ, D — дальність зв'язку СРЗ; V — швидкість передачі інформації в радіоканалі; C — перепускна здатність каналу радіозв'язку; Δt — час передачі інформації через канал СРЗ; $Z = \{z_1, z_2, \dots z_i, \dots z_I\}$ — множина видів МЗІ системи радіозв'язку.

Для військових СРЗ, які функціонують в умовах впливу інформаційних атак, оцінка ризиків ІБ повинна здійснюватись на двох етапах:

– функціонування;

– проектування.

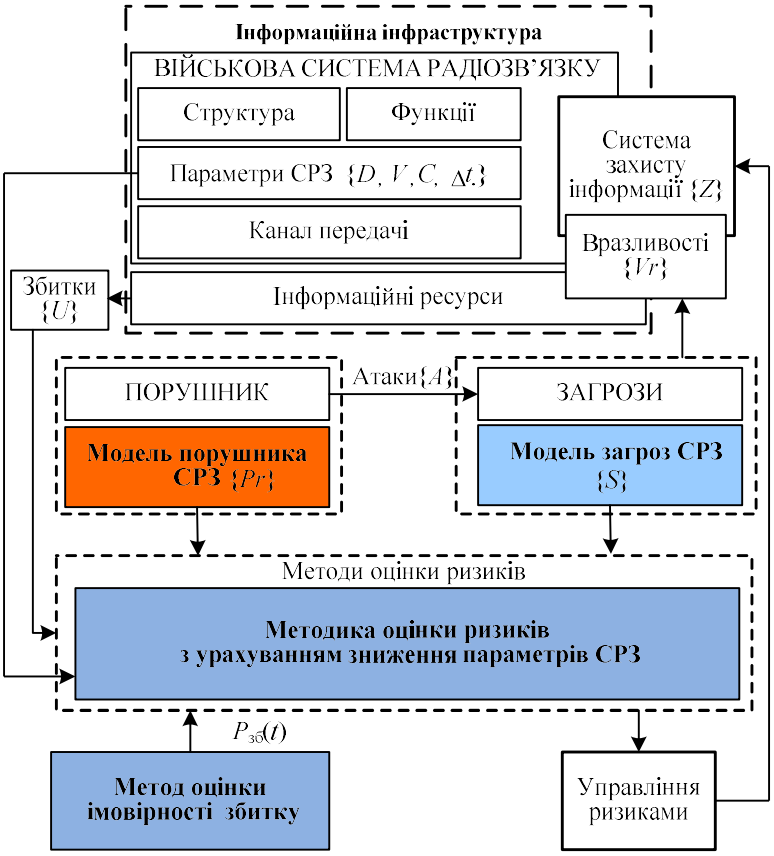


Рис. 1. Модель інформаційної безпеки військових систем радіозв'язку

На етапі функціонування, при впливі інформаційних атак, можливе застосування тих чи інших МЗІ, що в свою чергу знизять ризик ІБ. Відповідно до рис. 1, після розрахунку ризику здійснюється вибір МЗІ засобами керуючих впливів. Основна проблема лежить в тому, що ресурси захисту обмежені і при відсутності адекватних загрозам МЗІ це може призвести до втрат інформаційних активів.

На цьому фоні досить важливою є задача оцінки інформаційної безпеки на етапі проектування військових СРЗ.

Технологічно при проектуванні захищених СРЗ необхідно здійснити:

– оцінку ризиків з використанням відповідних МЗІ;

– вибір ефективних МЗІ, які дозволяють досягти більшого рівня захищеності інформації;

– оцінити рівень обмеження параметрів СРЗ внаслідок застосування МЗІ.

Враховуючі міжнародні підходи до управління ІБ були розроблені методи, що дозволяють здійснити оцінку ІБ військових СРЗ, на основі оцінки ризиків (рис. 2).

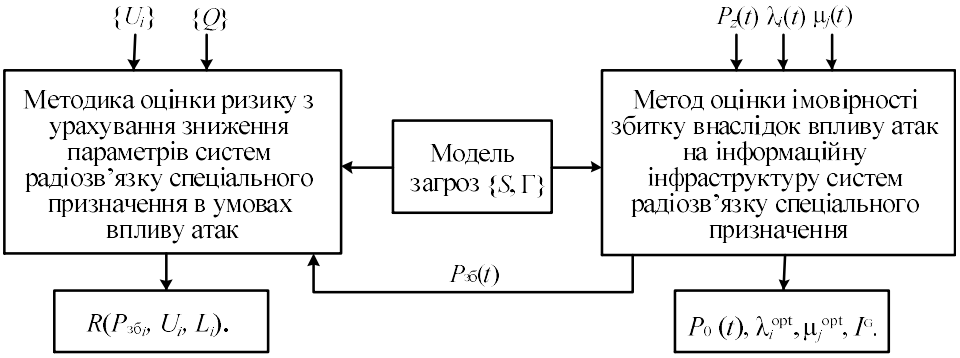


Рис. 2. Методи оцінки безпеки інформаційної інфраструктури СРЗ спеціального призначення в умовах впливу інформаційних атак.

Вихідними даними для оцінки ІБ інформаційної інфраструктури військових СРЗ та безпосереднього оцінювання ризиків на етапі проектування є дані про:

порушника $\{Pr\}$ (противника) та його можливості;

типи атак $\{A\}$, які порушник може реалізувати;

параметри СРЗ $\{Q\}$, що обмежуються внаслідок впровадження МЗІ від атак;

характеристики інформаційного конфлікту (стани в яких перебуває СРЗ при впливі інформаційних атак $P_z(t)$, інтенсивності дій сторін, що атакує та захищається — $\lambda_i(t)$, $\mu_j(t)$);

множину збитків $\{U\}$ внаслідок успішної реалізації атак.

В основі методів оцінки безпеки інформаційної інфраструктури військових СРЗ лежить модель загроз, яка враховує загрози від реалізації основних інформаційних атак на фізичний та канальний рівні СРЗ: перехоплення радіосигналу, перехоплення через технічні канали витоку інформації, проникнення до контрольованої зони, порушення управління СРЗ, передача дезінформації, радіоелектронне придушення (РЕП), деструктивний вплив, порушення системи захисту інформації СРЗ. Модель загроз враховує та описує основні інформаційні атаки на інформаційну інфраструктуру СРЗ, послідовність їх реалізації, критичні об'єкти інформаційної інфраструктури, кількісні показники інформаційних атак [1].

Так на рис. 3 представлена функціональна модель загроз інформаційної інфраструктури військових СРЗ в умовах впливу інформаційних атак, що відображає загрози та об'єкти впливу.

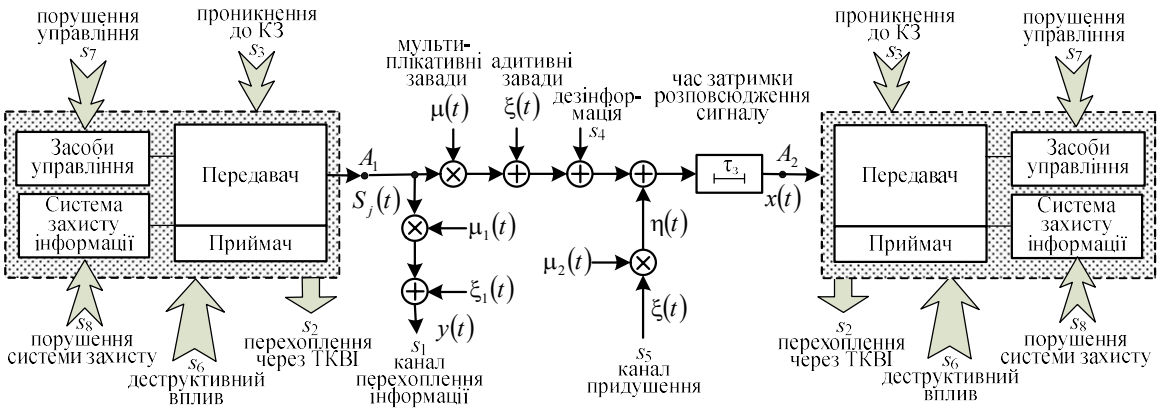


Рис. 3. Функціональна модель загроз інформаційної інфраструктури військових СРЗ в умовах впливу інформаційних атак

На етапі проектування СРЗ стоять два основних завдання: вибір ефективного МЗІ адекватного загрозам інформації; врахування впливу захисних функцій МЗІ на погіршення параметрів СРЗ.

Перше завдання на етапі проектування вирішується шляхом застосування диференційно-ігрового моделювання з можливістю зміни стратегій гравців інформаційного конфлікту. Метод оцінки імовірності збитку $P_{зб\,i}(t)$ дозволяє врахувати можливу динаміку зміни стратегій як порушника $\lambda_i(t)$, так і системи захисту інформації $\mu_j(t)$. Даний підхід дозволяє здійснювати порівняння та оцінку ефективності систем захисту інформації СРЗ в умовах впливу інформаційних атак та детально викладені в статтях [2]–[4].

Наступне завдання, досить важливе на етапі проектування, визначає на скільки обмежують МЗІ параметри СРЗ, що позначається відносним показником зниження *i*-ого параметру. Результат обмеження параметрів СРЗ впливає на зниження доступності інформації, що в свою чергу є додатковим ризиком ІБ *R* [5].

Для прикладу приведемо результати імітаційного моделювання при сумісному застосуванні методу оцінки імовірності збитку та методики оцінки ризику з урахуванням зниження параметрів СРЗ. На рис. 4 представлені результати моделювання зміни функції імовірності збитку при зміні інтенсивності гравців інформаційного конфлікту з кроком в 0,1 відносно рівноважних значень. При збільшенні інтенсивності захисних дій зменшується імовірність збитку, при збільшенні атаки противника — імовірність збитку збільшується. Вихідні дані, отримані за результатами імітаційного моделювання зміни імовірності збитку під час реалізації атаки РЕП, є вхідними даними для імітаційного моделювання зміни рівня ризику в умовах РЕП при зміні виду модуляції УКХ радіостанції в різних завадових станах (рис. 5). Так, при зменшенні швидкості передачі виникає додатковий ризик зниження доступності інформації, що відповідно впливає на збільшення загального рівня ризику інформаційної безпеки.

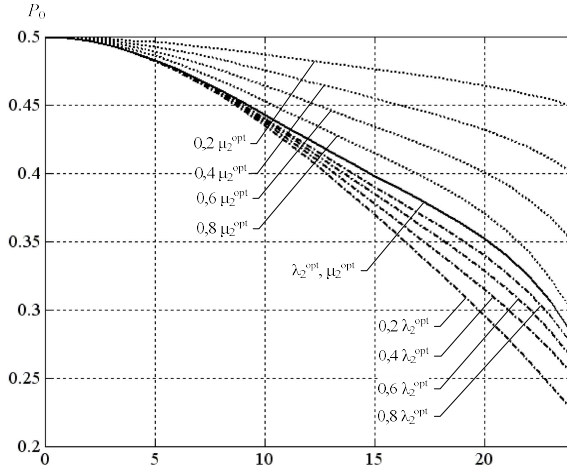


Рис. 4. Графіки зміни імовірності збитку СРЗ під час РЕП радіоліній СРЗ.

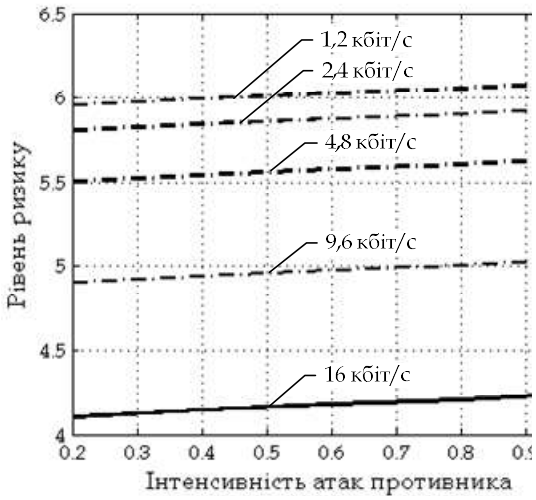


Рис. 5. Залежність рівня ризику від показника зниження швидкості передачі УКХ радіостанції при застосуванні завадозахищеного режиму.

В цілому розроблений метод та методика дозволяють повністю інтегруватись у загальну модель управління інформаційною безпекою та дозволяють оцінювати ризик безпеки інформаційної інфраструктури військових СРЗ на етапі проектування з урахуванням функціонування в умовах впливу інформаційних атак, що дозволить підвищити їх захищеність в умовах впливу інформаційних атак.

Список використаних джерел:

1. Шевченко А. С. Модель загроз для відомчих безпроводових інформаційно-комунікаційних систем в умовах інформаційної боротьби при впливі комплексу навмисних атак порушника / А. С. Шевченко // Сучасний захист інформації. — 2011. — № 3. — С. 58–65.

2. Шевченко А. С. Модель процесу перехоплення радіосигналів безпроводових інформаційно-телекомунікаційних систем в ході інформаційної боротьби / А. С. Шевченко // Сучасний захист інформації. — 2012. — № 3. — С. 43–50.

3. Шевченко А. С. Модель процесу придушення радіоліній безпроводових інформаційно-телекомунікаційних систем під час інформаційної боротьби / А. С. Шевченко, О. Є. Мазулевський // Сучасний захист інформації. — 2012. — № 4. — С. 35–40.

4. Шевченко А. С. Диференційно-ігрові моделі поведінки безпроводових інформаційно-телекомунікаційних систем при реалізації двоетапних атак під час інформаційного конфлікту / А. С. Шевченко // Збірник наукових праць ВІТІ НТУУ «КПІ». — 2012. — № 2. — С. 96–106.

5. Шевченко А. С. Метод оцінювання ризиків з урахуванням впливу механізмів захисту інформації на параметри безпроводових інформаційно-телекомунікаційних систем під час інформаційних операцій / А. С. Шевченко, О. В. Кокотов // Науково-практичний журнал «Безпека інформації». — 2014. — № 1. — С. 7–11.

УДК 004.056.5

[*]О.К. Юдін, [**]С.С. Бучик

**Національний авіаційний університет*

e-mail: ksz i@ukr.net

*** Житомирський військовий інститут імені С. П. Корольова*

Державного університету телекомунікацій

e-mail: s_stbu@ukr.net

УКРАЇНСЬКИЙ СЕГМЕНТ ДЕРЕВА ІДЕНТИФІКАТОРІВ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

В умовах стрімкого зростання новітніх технологій, подальшого розвитку інформаційного суспільства держави провідну роль відіграють її ресурси, а також система організації і вільного доступу до них всіх категорій суб’єктів

інформаційної діяльності. Державні інформаційні ресурси (ДІР) набувають базової значимості при реалізації процесів глобалізації інфраструктур, а також в умовах інтеграції України до світового інформаційного простору.

Ідентифікатори об’єктів (ІО) представляють собою певну схему ідентифікації для фізичних або віртуальних одиниць, яка заснована на деревоподібній структурі атрибутів ідентифікації, яку називають «Деревом міжнародного ідентифікатора об’єктів». Дерево складається з набору вузлів, починаючи з кореневого вузла. Від кожного вузла відходить довільна множина дуг, кожна з яким з’єднана з єдиним дочірнім вузлом на наступному рівні. Кількість рівнів дерева не обмежується.

Автори пропонують свою скореговану пропозицію для визначення і тлумачення ІО.

Ідентифікатор об'єкта (object identifier) — значення вузла, що відрізняється від інших подібних значень та логічно пов'язується з інформаційним об'єктом, унікально його визначає та однозначно ідентифікує, як вузол дерева міжнародних ідентифікаторів об'єктів. Список значень вузлів дерева (Root) є впорядкована послідовність первинних цілих значень, що починаються від кореня міжнародного дерева до вершини або/чи вузла ідентифікації.

Розглядаючи питання пов’язані з Національним реєстром електронних інформаційних ресурсів, Реєстром інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем не можливо уявити без їх відповідності до світового простору ІО. Зараз, український сегмент присутній, але він тільки конструктивно зазначений, наявність ідентифікаторів об’єктів Українського сегменту доволі незначна. Подібні процеси спостерігаються і при наповненні Національного реєстру та Реєстру інформаційних систем. Обидва реєстру мають фонд якій містить інформацію про державні електронні інформаційні ресурси. Однак, з цього напряму повністю відсутня система та рекомендації щодо процедур обов’язкової реєстрації державних електронних ресурсів. Проблема полягає і в тому, що функції управління основних реєстрів за нормативно-організаційними вимогами здійснюють різні структури, що свідчить про неузгодженість нормативно-правової бази. Існує гостра необхідність зосередження системи державного управління на базі одного органу. На думку авторів та у відповідність до законодавчої та нормативно-правової бази, враховуючі функціональні можливості і обов’язки — це Адміністрація Держспецзв'язку України. Дійсно, актуальною є задача реєстрації, накопичення й відображення систематизованої інформації про державні інформаційні ресурси, як в Національному реєстрі, Реєстрі інформаційних систем так і в реєстрі Світового простору ідентифікаторів об’єктів, гілка якого визначена для Українського сегменту.

Враховуючи вище наведений матеріал стосовно недоліків організаційної системи в країні з даного напрямку констатуємо, що робота майже не проводиться, немає узгодженості між наповненням реєстрів та єдиним органом управління.

Баранник В.В., Комолов Д.И., Тарнополов Р.В., Отман Шади О.Ю.

МЕТОДОЛОГИЯ СЕЛЕКТИВНОЙ ЗАЩИТЫ ВИДЕОПОТОКА ПО БАЗОВЫМ КАДРАМ ДЛЯ ВЕДОМСТВЕННЫХ СИСТЕМ

В ведомственных телекоммуникационных системах процесс шифрования может быть реализован на разных этапах формирования, обработки и передачи видеоданных, а именно: до сжатия видеопотока; после того, как сформировано компрессионное представление видеоданных; в процессе сжатия. Предлагается использовать вариант, в котором данные закрываются в процессе их сжатия — селективный подход. Такая реализация применяется в случаях обработки и передачи данных в системах реального времени (например, видеоконференцсвязь, где возможна дополнительная программная и аппаратная интеграция в видеокодек). Для такого варианта сжатие и шифрование выполняются для исходных данных по мере поступления их на обработку.

Реализация селективного подхода шифрования возможна на различных уровнях формирования MPEG-потока.

Предлагается закрывать только базовый I-кадр для уменьшения объема шифрованных сжатых видеоданных.

Основная часть. Наиболее значимым является I-кадр, так как в нем содержится максимальный объем несжатой информации, и кадры других типов содержат до 70% ссылок на него. Поэтому к дальнейшему рассмотрению предлагается совершать все манипуляции с I-кадром.

Были проведены экспериментальные исследования по шифрованию алгоритмом ГОСТ базового кадра. Брался I-кадр с различным качеством (34%, 67%, 100%), разными значениями пикового отношения сигнал/шум и коэффициентами степени сжатия, который подвергался шифрованию алгоритмом ГОСТ после квантования (в процессе сжатия). После чего предпринимались попытки восстановления его дифференцированного представления (B-кадра) при закрытом базовом I-кадре.

Объем сжатых видеоданных зависит от коэффициента сжатия, который является основной характеристикой алгоритма сжатия и определяется как отношение объёма исходных несжатых данных к объёму сжатых.

Коэффициент сжатия для кадров разных типов будет различным из-за использования разных технологий компрессии. Соответственно коэффициент сжатия для I-кадров будет самым низким из-за их большой насыщенности. Коэффициент сжатия для P-кадров выше, чем для I-кадров, но меньше, чем для B-кадров. Коэффициент сжатия для B-кадров будет самым высоким из-за меньшей степени квантизации и формата цветового представления.

Суммарный объем конкретного типа кадров в группе кадров зависит от их количества в группе кадров и от коэффициента сжатия, и не зависит от объема этих кадров.

Вывод. Исследования показали, что объем базовых I-кадров занимает от 20% до 60% всего объема видеопотока в зависимости от пиковых отношений сигнал/шум. Также наглядно представлено разрушение P-кадров при попытке их восстановления в случае закрытия I-кадра. Это указывает на то, что I-кадр значимо влияет на остальные кадры в группе. При закрытии базового кадра разрушается вся цепочка видеопотока. Таким образом, закрыв около от 20% до 60% видеоданных, достигается скрытие 100% передаваемой информации. При этом достигается экономия времени на обработку и передачу видеоданных. Полученные результаты показали, что в результате закрытии базового I-кадра, его объем увеличивается на 6-30% в зависимости от пикового отношения сигнал/шум. При высоком качестве исходного видеопотока, разница между объемом сжатых и закрытых сжатых видеоданных не значительна. Поэтому, селективный подход с закрытием базового I-кадра следует рассматривать для дальнейшего применения в ведомственных телекоммуникационных системах для обеспечения целостности, конфиденциальности и оперативной доставки высококачественных видеоинформационных ресурсов.

УДК 321.4

ВАВДІЧИК М.І.

Київський національний університет імені Тараса Шевченка,
mhlvdchk@gmail.com (М. І.)

АНАЛІЗ ГЕНЕРАТОРУ ШУМУ МЕРЕЖ ЖИВЛЕННЯ

Розглядається спосіб захисту інформації від витоку технічними каналами зв’язку. Обрання методів захисту є одним з найважливіших завдань у загальному комплексі заходів, щодо забезпечення від витоку інформації електричними каналами по колах електроживлення.

Аналіз [1] показує, що технічні канали витоку інформації можуть виникати за рахунок:

- Витоку з електричних мереж зв'язку;
- Витоку інформаційних сигналів в колах електроживлення технічних засобів обробки інформації;
- Витоку інформаційних сигналів в коло заземлення технічних засобів обробки інформації.

Проведено детальний аналіз каналу витоку інформації по колах електроживлення.

Поява інформаційних сигналів в колах електроживлення технічних засобів, пов'язаних з обробкою і передачею інформації, найчастіше обумовлено тим, що вони підключені до загальних ліній живлення. У будь-якому радіотехнічному виробі є власний блок живлення, що перетворює вхідну напругу від електромережі в необхідні для роботи напруги постійного або змінного струму. Небезпечний сигнал може за певних умов проникати через кола живлення приладу в мережу електроживлення приміщення, потім через силовий щит, розподільний пристрій за межі будівлі.

Розглянуто методи витоку інформації по колах електроживлення [2]. Для вирішення цього завдання можуть бути використані наступні методи і засоби:

застосування засобів та/або елементів гальванічної розв’язки кіл електроживлення, засобів призначених для обробки інформації з обмеженим доступом, з колом електромережі, застосування пристроїв автономного електроживлення на час оброблення інформації з обмеженим доступом засобів призначених для обробки інформації з обмеженим доступом, зашумлення кіл електроживлення засобів призначених для обробки інформації з обмеженим доступом.

Проведено порівняльний аналіз побудови та використання генераторів шуму для мереж електроживлення на прикладі:

ЛГШ-505 призначений для активного захисту об'єктів інформатизації від витоку інформації по мережі електроживлення 220 В 50 Гц («фаза», «нуль» і «захисне заземлення») Створює широкосмугові шумові електромагнітні перешкоди в діапазоні частот від 0,01 МГц до 1000 МГц [3].

ГНОМ-3М — стаціонарний генератор шуму для радіотехнічного маскування і захисту кіл електроживлення [4].

Комплекси П220 — універсальні генератори шуму, призначені для активного захисту об'єктів інформатизації шляхом маскування побічних електромагнітних випромінювань і наведень (ПЕМВН) шумовими сигналами.[5]

Генератор Марс –ТЗО. Генератор призначений для створення шумового сигналу в діапазоні частот від 180 до 5600 Гц при використанні у складі технічних засобів активного захисту інформації від витоку з об'єктів акустичним і віброакустичним каналами. Шумовий сигнал формується генератором псевдовипадковії послідовності з періодом повторення більше 24 год.

Детально проведено дослідження *Генератору Марс –ТЗО.* Для отримання параметрів шумового сигналу (електричні процеси у генераторі, в яких діапазонах відбувається генерація шумового сигналу та інші) використовувався спектроаналізатор *Tektronix MDO4104-6*.

Аналіз генерування шуму проводився на виходах кожного каскаду схеми. При цьому застосовувався алгоритм швидкого перетворення Фур’є — інтегральне перетворення однієї комплексної функції дійсної змінної на іншу. Ця функція описує коефіцієнти («амплітуди») при розкладанні вихідної функції на елементарні складові — гармонійні коливання з різними частотами. Використовується для того, щоб розрахувати спектр частот для сигналів змінних у часі (таких як мова або електрична напруга). На рис.1 зображено блоксхему генератору шуму Марс ТЗО-СЗ. Для дослідження кожного вузлу необхідно було зняти осцилограми з їх виходів.

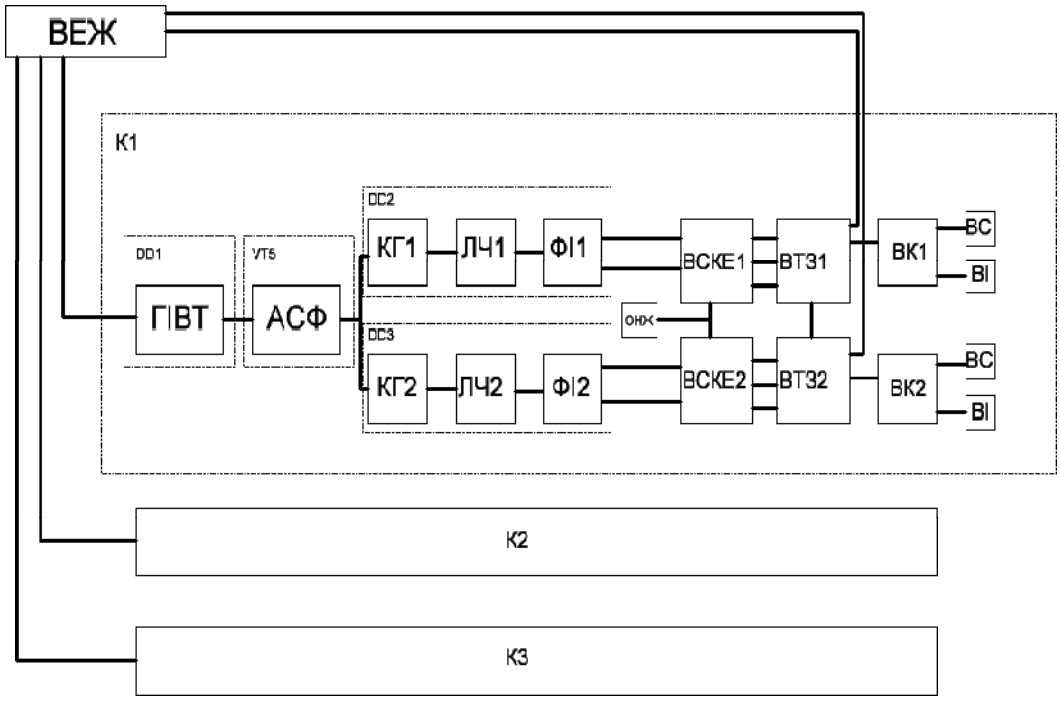


Рис.1 Блоксхема ГШ Марс –ТЗО-СЗ

Аналіз вузлу *ГІВТ* (генератору імпульсів випадкової тривалості показав, що періодичність слідування обвідної на більш низьких частотах сигналу шуму досить низька). Наступний вузол являє собою *АСФ* (активний смуговий фільтр). Імпульси, що поступають на вхід — перетворюються в аналоговий НЧ шумоподібний сигнал. АСФ виділяє частину спектру, що має нормальний розподіл спектральних складових шуму та подає його для подальшого перетворення на блок мікросхем DD2 DD3 (КР (КФ) 1211ЕУ1). Ці мікросхеми ідентичні і являють собою керований генератор, лічильник і формувач імпульсів. *Мікросхеми* формують пачки імпульсів однакової тривалості, які підсилюються каскадом на чотирьох польових транзисторах (вузол на ключових силових елементах). Осцилограми, зняті зі стоків цих транзисторів показують, що одна пара транзисторів працює з більш низькими частотами, а інша з більш високими. На рис.2 зображено спектральні характеристики, отримані з виходу ГШ. Отримана за допомогою трансформатора струму спектральна характеристика шумового сигналу показує, що гранична частота шуму знаходиться до 200кГц, тобто мовний електричний сигнал в мережі живлення [6] буде захищено.

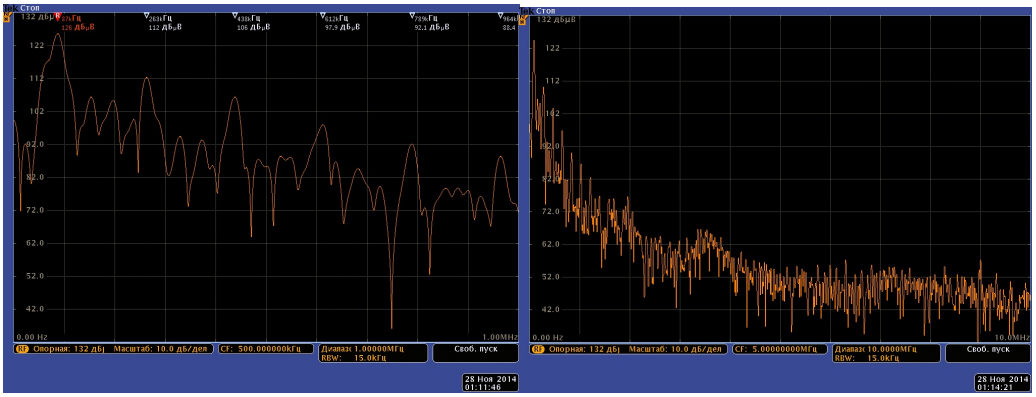


Рис.2 Спектральні характеристики на виході ГШ

Проведено дослідження генератору шуму «МАРС-ТЗО-СЗ» дозволило розробити напрями його удосконалення:

а) задаючий генератор сигналів побудувати на базі фізичних н/п пристроїв, наприклад напівпровідникових шумових діодів;

б) замінити формувачі імпульсів керування силовими ключами шумових сигналів на інші в яких відсутній лічильник;

в) забезпечити формування широкосмугових шумових сигналів, що мають монотонні спектральні характеристики за рахунок застосування багатокаскадних схем генерування шумових сигналів та їх подальшого матричного синтезу.

Литература:

1. http://mordvinovoe.narod.ru/220v.htm
2. Максимов Ю. Н., Сонников В. Г., Петров В. Г. и др. Технические методы и средства защи-ты информации. — СПб.: ООО «Издатель-ство Полигон», 2000. — 320 с.
3. http://www.pps.ru/?part=catalog&product=95
4. http://www.sis-tss.ru/2010-06-24-20-02-16/5746-statsionarnyj-generator-shuma-dlja-radiotehnicheskoj-maskirovki-i-zaschity-tsepej-elektropitanija-gnom-3m.html
5. http://kalugapribor.ru/produce/p220.html
6. http://soundtheory.northsoundrecords.com/home-vocal-recording/

Научный руководитель — кфмн., В.Ф. Борецький

Васильєва В.О., студ., Розорінов Г.М., проф., Чичикало Н.І., проф.

ДЖЕРЕЛА ВИНИКНЕННЯ ПОХИБКИ ТА ОЦІНКА СТУПЕНЮ ЇХ ВПЛИВУ НА ХАРАКТЕРИСТИКИ РАДІОКАНАЛУ

При реалізації моделей з використанням радіоканалу основні джерела погрішностей виникають через невідповідність основних показників елементів, використовуваних в практиці.

Потужність сигналу приймача $P_{прм}=\frac{P_{пер}\cdot D_{пер}\cdot D_{прА}\cdot \eta_{пер}\cdot \eta_{прм}\cdot \lambda^2}{(4\pi R)^2}$, де $P_{пер}$ — потужність передавача; $D_{пер}$ — КСД (коефіцієнт спрямованої дії) передавача; $D_{прА}$ — КСД приймача; $\eta_{пер}$ — коефіцієнт корисної дії тракту передавача; $\eta_{прм}$ — коефіцієнт корисної дії тракту приймача; λ^2 — довжина хвилі; R — відстань. Оцінимо, як змінюватиметься потужність сигналу приймача залежно від зміни коефіцієнта стоячої хвилі (КСХ) і загасання фідера на передавачі і приймачі, а також як впливає погрішність параметрів КСХ.

КСХ характеризується міра узгодження антени з лінією фідера:

$$\text{КСХ} = \frac{U_{max}}{U_{min}}.$$

На рис. 1 представлена залежність потужності на вході приймача від КСХ антени. Для ідеально погодженої антени КСХ=1. Реально у добре погодженої антени КСХ≤ 1,2÷1,5. Зі збільшенням погрішності значення потужності зменшується.

Оцінемо вплив погрішності загасання фідера приймальної і передавальної антен на вхідну потужність приймача. На рис. 2 показана залежність потужності на вході приймача від загасання у фідерах приймальної і передавальної антен.

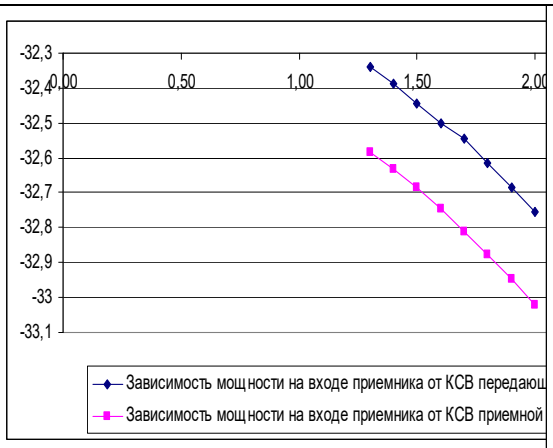


Рис .1. Залежність потужності на вході приймача від КСХ антени

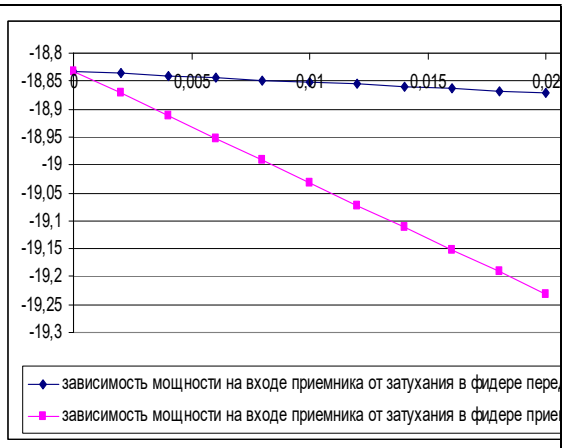


Рис.2. Залежність потужності на вході приймача від загасання у фідерах передавальної і приймальної антен

Висновки

1. Показано, що в залежності від зміни КСХ і загасання фідера на передавачі і приймачі, збільшення КСХ і загасання у фідері призводить до зменшення потужності сигналу.

2. Зменшення потужності сигналу можуть виникати через несправність передавального і приймального тракту, оскільки КСХ антен збільшується при несправності, а так само і загасання фідера при його ушкодженні, тобто відхиляється від якогось стандартного значення.

Я.Ю. Власенко студ., О.Д. Василенко ст. вик.

Національний технічний університет України «Київський політехнічний інститут» mazay@forenet.info

МОЖЛИВІСТЬ ВИКОРИСТАННЯ МОДЕРНІЗОВАНИХ ПІЧ-ДЕТЕКТОРІВ У ЯКОСТІ «КВАЗІТЕПЛОВІЗОРІВ»

На сьогодні ПІЧ- детектори є невід'ємним елементом охоронної системи практично кожного об'єкта. Існує багато видів ПІЧ-детекторів руху які мають однотипну конструкцію та однакові недоліки — детектор руху спрацьовує тільки на рух об’єкта, який потрапляє в зону виявлення. Коли об’єкт (порушник) буде знаходитись у нерухомому стані або за перешкодами, такими як дерева, зелені насадження, фасадні конструкції, то ПІЧ -детектор руху не виявить його.

Існують інші прилади, такі як тепловізори, що дозволяють виявити нерухомий об’єкт, температура якого відрізняється від навколишнього середовища. Тепловізор — це оптико-електронна система, що формує з теплового (інфрачервоного) випромінювання об'єкта візуально видиме зображення. Чутливим елементом тепловізора є матриця — мікросхема з

набором піроелектричних приймачів. Ця матриця має формат, найбільш розповсюджений на сьогоднішній день, розмірністю від 128x128 до 640x512 елементів при розмірі цих чутливих елементів від 25 до 75мкм. Чутливість системи є прямо пропорційною до площі приймального елементу і розраховується за формулою[1]:

$$D = (A\Delta f)^{1/2}\frac{1}{P_{th}}$$

де A — площа чутливого елемента; Δf — ширина смуги пропускання електронного тракту посилення сигналу і шуму; P_{th} — енергетичний потік випромінювання, при якому відношення сигнал-шум дорівнює одиниці.

При однаковій питомій чутливості один піроелектричний приймач, з розміром чутливого елементавід 1x1мм до 8x8мм, які використовуються в сучасних ПІЧ-детекторах має явно більшу чутливість ніж один елемент матриці тепловізора при однаковій побудові системи виявлення. Крім того, складність та вартість останнього затрудняють його використання у якості звичайного елемента охоронної системи.

Тому доцільним є розглянути можливість побудови «квазітепловізора» з комплексу піроелектричних приймачів кожен з яких сприймає теплове випромінювання тільки з відповідного кута по азимуту. При обмеженні цього кута 1-2 град. такий пристрій має більшу чутливість ніж прототип, що збільшує здатність виявлення, а погіршення його характеристик при візуалізації виявленого теплового випромінювання перекривається меншою вартістю. Формування сигналу виявлення забезпечується за рахунок порівняння сигналів в різних кутах при скануванні по азимуту

Для визначення можливостей виявлення порушника за перешкодами, розглянемо реальний час, коли це виявлення можливе.

Оцінка теплового потоку де передача енергії відбувається між людиною та перешкодою, вираховується як [2]:

$$Q = F \cdot \alpha(T_1 - T_2) = 230 \text{ Вт}$$
$$\alpha = \varepsilon\sigma_0(T_1 + T_2)(T_1^2 + T_2^2) = 5{,}91 \text{ Вт/(м}^2 \cdot \text{К)}$$

σ_0 = 5,67 · 10^{-8} Вт/(м^2·К^4) — постійна Стефана-Больцмана; F — площа поверхні м^2 (тіло людини — 1.86м^2); ε — випромінююча здатність (для людського тіла — 0,98); T_1 — абсолютна температура К, для людини -309; T_2 — абсолютна температура К, для перешкоди -288.

Час при якому перешкода набуває температури порушника, який ховається за нею вираховується відповідно до[2]:

$$\tau = \frac{Q \cdot \delta}{\lambda \cdot (T_1 - T_2) \cdot S}$$

δ– товщина перешкоди (м); λ — коефіцієнт теплопровідності матеріалу перешкоди;

S — площа перешкоди.

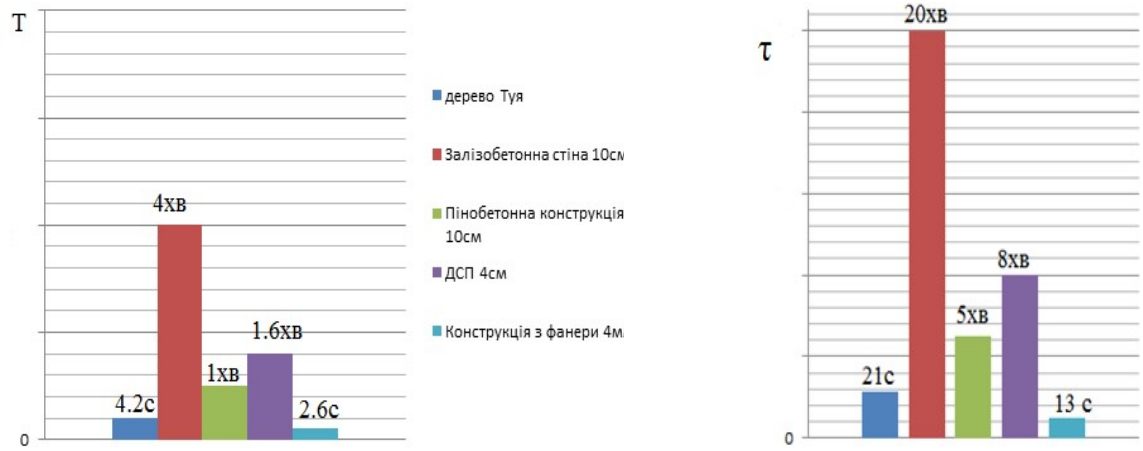
Розрахунок часу проведений при умові, що випромінювання від людини одночасно є фоном на певній дистанці та для перешкод, які є найбільш імовірними на площах, що охороняються: зелене насадження (хвойне дерево Туя, в більшості випадків саме це дерево висаджують на території яку потрібно захистити); стінка із залізобетону товщиною 10см; стінка з пінобетону товщиною 10см; конструкція з ДСП товщиною 4 см; конструкція з фанери товщиною 4мм.

За результатами розрахунків, побудована гістограма, що приведена на рис1б. На рис 1а наведені результати, що враховують можливість виявлення навіть в тому випадку, коли температура перешкоди тільки відрізняється від навколишнього фону, що потребує значно меншого часу, який для «квазітепловізора» у першому наближенні оцінюється, як:

$$T = \tau \cdot K_ч$$

$K_ч$ — коефіцієнт чутливості, для піроелектричного приймача становить 0,…1.

Для $K_{ч=}$ 0,2



а б

Рисунок 1 — Гістограма: а) часу за який «квазітепловізор» виявить зміну температури між об’єктом за перешкодою та навколишнім середовищем; б) часу при якому перешкода набуває температури порушника, який ховається за нею

Отримані результати показують, що людина — порушник може бути виявлена «квазітепловізором» навіть за перешкодами, коли його швидкість дозволяє за певний час нагріти перешкоду.

Список використаних джерел:

1. Груба И. И. Системы охранной сигнализации. Технические средства обнаружения / И.И Груба // библиотека инженера. 2012. — 220ст.

2. Круз.П Макглоумен Л. Основы инфракрасной техники / П. Круз, Л. Макглоумен//Воениздат — 1964 — 464с.

М.Ю. Власенко студ.,О.Д. Василенко ст. вик.,
Національний технічний університет України «Київський політехнічний інститут» mazay@forenet.info

РОЗШИРЕННЯ МОЖЛИВОСТЕЙ ДВОПОЗИЦІЙНИХ РАДІОПРОМЕНЕВИХ СИСТЕМ ВИЯВЛЕННЯ

На сьогоднішній день двопозиційні радіопроменеві системи виявлення (РПСВ) широко застосовуються при охороні периметрів об'єктів різного призначення як державної так і приватної власності. Такі засоби виявлення відносяться до незагороджувальних. Найчастіше вони використовуються як доповнення до огорож різного роду, а самостійно тільки як мобільні системи [1].

Недоліком таких систем є мала зона виявлення (від 2 до 5 метрів), що призводить в деяких місцях до підвищення ймовірності хибної тривоги. З метою усунення цього недоліку доцільно розширити зону виявлення, що унеможливить появу хибної тривоги при тих же характеристиках виявлення.

Можливим варіантом може бути використання сітки променів, за рахунок якої розшириться зона виявлення при тих же технічних засобах. Одним з таких варіантів для немобільних систем, які працюють безпосередньо поблизу огорожі, може бути використання спеціалізованих відбиваючих незаземлених дзеркал. (Рис 1) Відбивачі повинні бути розміщені таким чином, що б при куті відбивання промені потрапляли на приймач. Таким чином утворюється практично повністю перекрита площа зони за рахунок «сітки» променів що, по-перше збільшує зону виявлення, по-друге зменшує можливі хибні тривоги за рахунок того, що порушник рухаючись в зоні обов'язково буде перекривати не один, а декілька променів в різний час за один прохід.

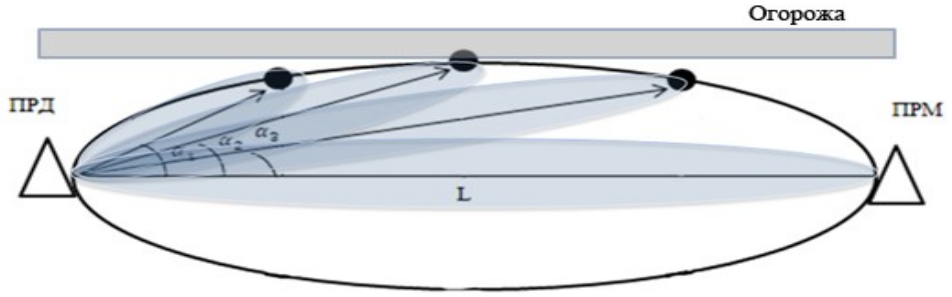


Рисунок 1 — РПСВ з багатопроменевою антеною та відбивачами

Реалізація такої системи можлива в двох напрямках:

1) Синхронізовано змінними кутами як передавача, так і приймача.

2) Випромінювач змінює спрямованість, а система приймання з широким променем залишається незмінною.

При частотах, які, зазвичай застосовуються в РПСВ — від 10 до 50 ГГц-антенні системи можуть бути як з фазованою решіткою, так і звичайні.Аналіз застосування відповідних реалізацій РПСВ з тими чи іншими антенами показує, що при використанні антенних решіток краще використовувати напрямок реалізації 1, при звичайних доцільніше напрямок 2.

Вузли передавача і приймача повинні бути засинхронізовані тому, що і в першому і в другому випадках випромінювання і приймання в різних променях відбувається в різний час. Це дозволяє визначити не тільки площу в зоні

виявлення де знаходиться порушник, але й при відповідній обробці сигналів інформаційні параметри порушника — його швидкість, напрямок пересування.

За рахунок того,що при відбиванні від дзеркал характер сигналу відрізняється від сигналів у звичайних лінійних РПСВ його обробка в приймальному вузлі при визначенні факту перетину у відбитих променях повинна також відрізнятись від обробки сигналів без відбиття [2].Застосування таких модифікованих систем дозволяє розширити зону виявлення з 2…5 метрів до 10…15м та за рахунок інтегральної обробки сигналівдає змогу знизити ймовірність хибної тривоги (підвищення часу напрацювання на хибну тривогу) та підвищити ймовірність виявлення порушника у розширеній зоні..

Список використаних джерел:

1. Груба И. И. Системы охранной сигнализации. Технические средства обнаружения / И.И Груба // библиотека инженера. 2012. — 220ст.

2. Звежинский С.С. Средства обнаружения исистемы охранной сигнализации: Учебное пособие длявузов/ С.С.Звежинский, В.А.Иванов // М.: МТУИ, 2008 — 260с

УДК 621.396.962

В.В.Войтко, А.І.Ільницький

Військова частина А1906

Інститут телекомунікаційних систем НТУУ «КПІ»,

кандидат технічних наук, доцент, с.н.с.,

its@ntu-kpi.kiev.ua

ПРОБЛЕМНІ ПИТАННЯ МОНІТОРИНГУ ДЖЕРЕЛ РАДІОВИПРОМІНЮВАННЯ СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ТА НАПРЯМИ ЇХ ВИРІШЕННЯ

Інформаційна безпека є однією з багатьох складових національної безпеки і оборони будь-якої світової держави. На сьогодні, в умовах загострення зовнішньої та внутрішньої воєнно-політичної обстановки на Україні особливу актуальність набуває забезпечення інформаційної безпеки та підтримки прийняття управлінських рішень з використанням результатів моніторингу джерел радіовипромінювання (ДРВп) телекомунікаційних систем і мереж (ТСМ) різного призначення. При цьому обов’язковим є отримання і використання результатів експрес-аналізу радіоелектронної обстановки (РЕО) у територіальних межах держави і за її кордоном. Як показує практика, при веденні моніторингу ТСМ у мирний та воєнний часи РЕО постійно ускладнюється і характеризується такими основними факторами:

постійним зростанням кількісного та якісного складу ДРВп на фоні обмежених ресурсів наявних сил і засобів радіомоніторингу, що зменшує ефективність їх застосування;

дуже широким частотним діапазоном сигналів ТСМ (від 30 МГц до 100 ГГц) з тривалістю вхідних сигналів від десятків нс до сотень мкс;

щільним потоком сигналів ТСМ у точках їх прийому — 10^5-10^7 імп/сек;

застосуванням у ТСМ сигналів зі складною частотно-часовою структурою та інформаційним наповненням і використанням прихованих режимів роботи з короткочасними сеансами випромінювання, що значно ускладнює аналіз їх параметрів і характеристик та збільшує час обробки інформації тощо.

У доповіді надається характеристика змісту науково-технічних проблемних питань і суперечностей, які виникають у наведених умовах, а також звернута основна увага на забезпечення високої точності, достовірності, надійності і швидкодії вимірювань та аналізу параметрів сигналів ДРВп ТСМ різного призначення. Зроблено висновки, що існуючий стан сил і засобів радіомоніторингу державних установ та їх науково-теоретична і технічна бази не забезпечують у повному обсязі вирішення завдань за призначенням у реальному масштабі часу в умовах повної або часткової невизначеності параметрів сигналів. На підставі наведеного сформульовані напрями вирішення існуючої проблемної ситуації і суперечностей та основні наукові і практичні завдання, які спрямовані на підвищення ефективності об'єкта дослідження. Як практичний приклад, з урахуванням введених обмежень і вихідних даних, розглядаються наукові і практичні пропозиції щодо шляхів визначення та вимірювання енергетичних, частотно-часових, просторових та інформаційних параметрів сигналів ДРВп ТСМ в умовах часткової невизначеності. При цьому у доповіді основна увага надається вирішенню питань моноімпульсного миттєвого аналізу (за час тривалості одного імпульсу сигналу) за рахунок розробки нових й удосконалення існуючих математичних (імовірнісних) моделей, методів і методик, процедур та способів вимірювання параметрів і визначення характеристик ДРВп. Для наочності наведені результати удосконалення математичної імовірнісної моделі (нові аналітичні залежності) процесу визначення і вимірювання миттєвої частоти простих імпульсних сигналів та структурно-функціональна схема двоканального вимірювача, яка синтезована за розробленим методом моноімпульсного вимірювання частоти.

Як підсумок наведені висновки, що характеризують отримані наукові і практичні результати, та визначено напрями подальших досліджень у предметній області, що розглядається.

УДК 004.5

Е.С. Воронкова, Д.Д. Фокин

Физико-Технический Институт НТУУ «КПИ» pti@pti.kpi.ua

КОЖНО-ГАЛЬВАНИЧЕСКИЕ РЕАКЦИИ В СОВРЕМЕННЫХ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЯХ

Рассматривается проблема биометрической идентификации и аутентификации пользователя информационно-коммуникационной системы. Цель работы — нахождение способов улучшения методов идентификации и аутентификации.

Актуальность применения биометрических технологий обусловлена большей надежностью их защиты по сравнению с методами ключей и паролей в силу привязки к биометрическим характеристикам конкретного человека. Такая функция вегетативной нервной системы, как потоотделение, также дает возможность для анализа психологических феноменов. Результаты многочис-

ленных исследований позволили предположить, что кожно-гальваническая реакция (КГР) отражает эмоциональные реакции, возможно, не осознаваемые человеком. На этом предположении основано использование детектора лжи.

В рамках описываемого исследования проведён следующий эксперимент. Сконструирован датчик КГР (методика Тарханова) и надет на испытуемых. Команде из десяти человек было предложено создать аккаунт в общей сети, требовавший заполнения полей «логин» и «пароль». Каждому испытуемому по отдельности сообщили данные другого участника эксперимента, но уточнили, что использовать чужие данные запрещено. На следующий день эксперимента всем испытуемым было предложено зайти в аккаунт другого человека.

Проанализированы полученные экспериментально усреднённые данные КГР десяти человек, которые проходили правдивую и ложную авторизацию (рис.1). Как видно из приведенных графиков, в первом случае кривая КГР слабо колеблется относительно среднего уровня, когда же во втором случае заметно значительное падение амплитуды КГР.

Таким образом, при оснащении персональных устройств датчиками, измеряющими электродермальную реакцию, существенно повышается эффективность методик аутентификации и идентификации.

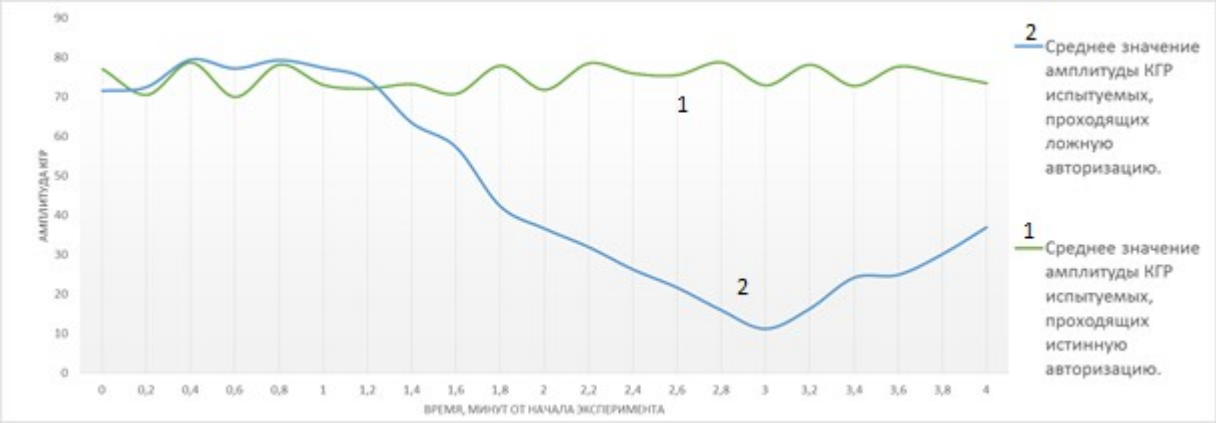


Рисунок 1. — Результат эксперимента.

Научный руководитель — д.т.н, проф. Е.А. Мачуский.

Двухглавов Д.Э., Твердохлеб В.В., Ларин В.В., Мусиенко А.П.

АЛГОРИТМ СЖАТИЯ ВИДЕОПОТОКА С ИСПОЛЬЗОВАНИЕМ БИТОВОГО КУБА

Одним из актуальных направлений решения задачи обеспечения заданного уровня качества видеоданных является снижение времени передачи данных путем снижения объема передаваемых данных. Формализованная постановка данной задачи предполагает отыскание минимума битовой скорости, представляющей собой объем сжатых видеоданных, которые требуется передать в единицу времени, при заданной степени достоверности передачи данных видеокадра, относительно исходного, выраженной среднеквадратическим отклонением (СКО).

При сжатии видеопотока кадры разбиваются на блоки, каждый из которых далее подвергается обработке в соответствии с заданным алгоритмом. Часть алгоритмов, прежде всего JPEG, на начальных этапах обработки

предполагают преобразование исходного фрагмента из модели **RGB** в модель $\mathbf{YC_bC_r}$, после чего к нему применяется дискретно-косинусное преобразование (**ДКТ**). После данных обязательных шагов выполняется кодирование полученной трансформанты с использованием различных подходов. В тоже время следует обратить внимание на тот факт, что основная энергия исходного сигнала сосредоточена в определенном количестве низкочастотных компонент трансформанты, полученной после проведения ДКТ. Учет этого факт позволяет сформулировать гипотезу о том, что снижение времени передачи можно получить путем передачи только отдельных компонент трансформанты, при этом соблюдая требования к СКО.

Для реализации такого подхода предлагается представить каждую трансформанту в виде битового куба, который может быть получен путем представления каждого элемента трансформанты в виде столбца бит, соответствующего представлению компонента (i,j) в двоичной системе счисления. При этом верхний слой данного куба образуют старшие биты двоичного представления. Принято именно такое представление, так как потеря информации в верхних битах определяет большее искажение передаваемого блока на приемной стороне.

Такое представление трансформанты обеспечивает возможность управления компрессией изображения. Сущность управления заключается в том, что при передаче можно передавать только часть слоев, тем самым уменьшая размер изображения. Количество возможных вариантов передачи слоев битового куба трансформанты $\boldsymbol{P}$ будет равно 256. Каждому варианту передаваемых слоев будет соответствовать изображение, соответствующее исходному, но различающиеся степенью искажения исходного изображения.

Чтобы определить слои, которые необходимо передать, предлагается задать для каждой трансформанты свой байт передачи. Если пронумеровать возможные варианты передачи от $\mathbf{1}$ до $\boldsymbol{P}$, то байт передачи соответствует двоичному представлению числа $\boldsymbol{p}-\mathbf{1}$.

Передаваемая последовательность для каждой трансформанты формируется в соответствии с алгоритмом:

1. Обнулить передаваемую последовательность бит трансформанты. 2. Добавить байт передачи. 3. Добавить биты слоя битового куба, которым соответствует 1 в байте передачи.

Длина кодовой комбинации будет составлять от 72 до 520 бит (от 9 до 65 байт).

Алгоритм сборки битового куба на приемной стороне из полученной последовательности предполагает следующие шаги: 1. Обнулить битовый куб. 2. Выделить из принятой последовательности байт передачи (первые 8 бит). 3. Заполнить элементы битового куба для слоев, которые соответствуют ненулевым битам в байте передачи, данными из последовательности (64 бита) или заполнить слой нулями.

Реализация такого подхода к передаче компрессии трансформанты кадра изображения сокращает время передачи за счет сокращения времени на кодирование элементов после ДКТ. Также в этом случае для обеспечения

значения СКО, не превышающего заданного, будет передаваться различное число бит, что позволит сократить объем передаваемых бит преобразованного исходного изображения, что, в свою очередь, обеспечит сокращение времени передачи видеопотока в целом.

УДК 321.4

ДОВБНЯ С.Я.,к.в.н., доцент, ШПИЛЬОВИЙ В.С., НІКОЛЬСЬКИЙ С. А.

Київський національний університет імені Тараса Шевченка,

ssnik50@yandex.ru

ОБРАННЯ ВИДУ АКУСТИЧНОГО ШУМУ ДЛЯ ЗАХИСТУ КОМЕРЦІЙНОЇ ІНФОРМАЦІЇ

В останні роки з розвитком комерційної і підприємницької діяльності збільшилось число спроб несанкціонованого доступу до конфіденційної інформації. Однією із задач захисту мовної інформації є забезпечення захисту від витоки через технічні канали. Обрання методів захисту є одним з найважливіших завдань у загальному комплексі заходів, щодо забезпечення інформаційної безпеки об’єкта або установи (рис.1, таблиця 1).

Для захисту мовної інформації використовують активні і пасивні методи захисту. До пасивних методів відносять екранування приладів, звукоізоляція приміщень, використання акустичних екранів. Активні засоби повинні забезпечувати зменшення співвідношення сигнал/шум за рахунок збільшення рівня шуму. Для захисту інформації від підслуховування використовуються генератори акустичної шумової перешкоди.

В сучасних АГШ найчастіше використовуються 3 види акустичного шуму:

• Білий шум — це сигнал з рівномірною спектральною щільністю на всіх частотах і дисперсією, рівної нескінченності. Такий сигнал має однакову потужність в однаковій смузі частот будь-якій частині діапазону.

Таблиця 1.

Мета захисту комерційної інформації	Категорія захисту ОІД	Можливі ТКВІ	Критерій ефективності захисту (розбірливість мови)Wn	Максимальне співвідношення сигнал/шум дБ
Укриття факту ведення переговорів	1 КТ	Акустичній, Віброакустичній, акустооптичній, акустоелектричній, акустоелектромагнитний	Wn ≤ 10%	Від -12 до -16
Укриття предмету переговорів	2 КТ		Wn ≤ 20%	Від -9 до -13
Укриття змісту переговорів	3 КТ		Wn ≤ 30%	Від -6 до -10
Укриття змісту переговорів	4 КТ	Акустичній (непередбачене прослуховування)	Wn ≤ 40%	Від -5 до -9

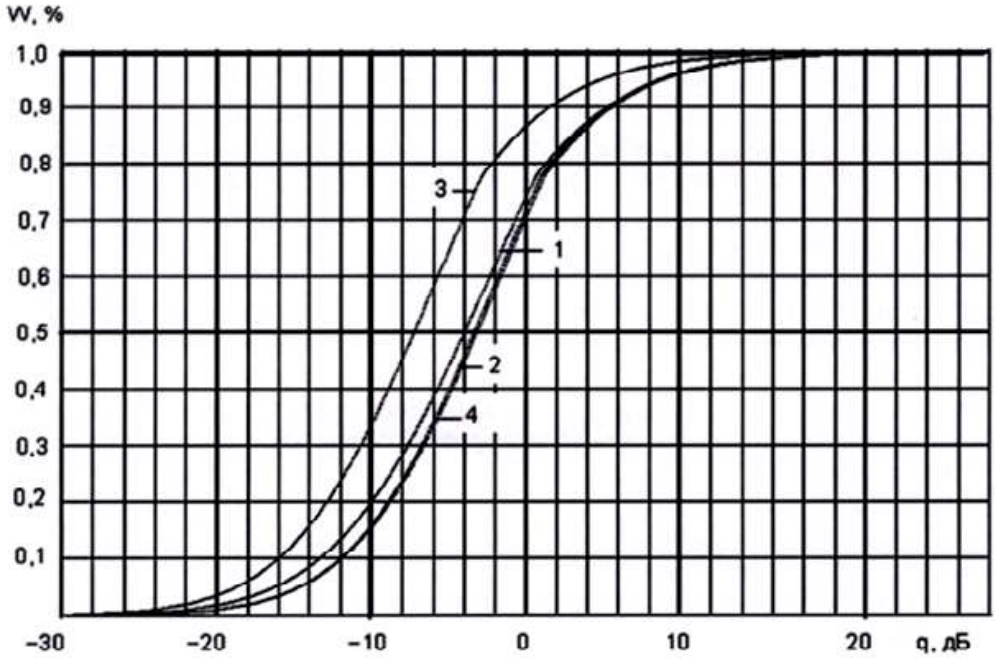


Рис. 1. Залежність словесної розбірливості W від інтегрального відношення сигнал/шум q в діапазоні частот 180-5600 Гц: 1 - "Білий шум"; 2 - Рожевий шум (шум зі спадом спектральної щільності 3дБ на октаву в бік високих частот); 3 - Шум зі спадом спектральної щільності 6 дБ на октаву в бік високих частот; 4 - Шумова "мовна" перешкода.

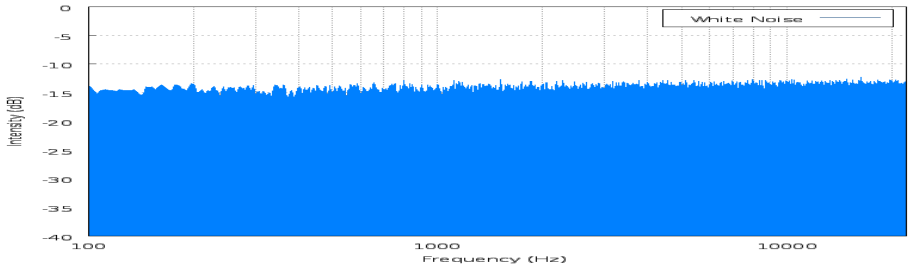


Рис.2 Спектр білого шуму

• Рожевий шум — спектральна щільність потужності шуму визначається ~ 1/f (щільність обернено пропорційна частоті), тобто він є рівномірно спадаючим в логарифмічною шкалою частот. Спектральна щільність такого сигналу в порівнянні з білим шумом затухає на 3 децибели на кожну октаву.

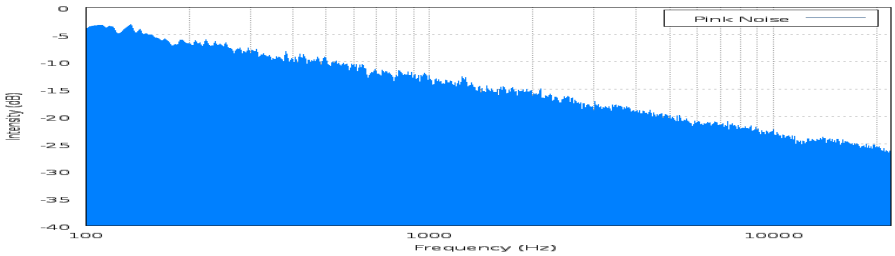


Рис.3 Спектр рожевого шуму

• Червоний шум (коричневий) — спектральна щільність шуму пропорційна $1/f^2$. Це означає, що на низьких частотах шум має більше енергії, ніж на високих. Енергія шуму падає на 6 децибел на октаву. Акустичний червоний шум чується як приглушений, в порівнянні з білим або рожевим шумом. На слух червоний шум сприймається більш «теплим», ніж білий.

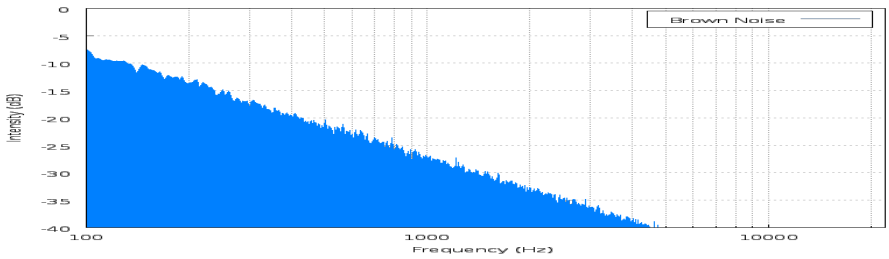


Рис.4 Спектр червоного шуму

В ході досліджень було проведено модулювання випромінювання АГШ різних завад.

Список використаних джерел:

1. Довбня С.Я., Кривцун В.І., Четверіков І.О., Савран В.О., Солдатенко О.О.

Науково-методичне забезпечення створення та функціонування системи інформаційної безпеки держави. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. — К.: ВІКНУ, 2014. — Вип. № 47. — с. 98-108.

2. Халяпин Д.Б., Рюмин А.А. Коктейль из звуков // «Information Security/ Информационная безопасность» -2005- №4- с28-29

3. Дворянкин С.В., Макаров Ю.К., Хорев А.А. Обоснование критериев эффективности защиты речевой информации // Защита информации. Инсайд. — 2007. — № 2. — С. 18 — 25.

УДК 004.056.5

С.Я.Довбня, к.в.н.

О.О.Солдатенко

Т.М.Підлипна

Київський національний університет імені Тараса Шевченка,

dovbnja.sergej@i.ua, Soldier_@ukr.net

НАУКОВО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ СТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Нині розвиток сучасних інформаційних технологій, під якими розуміються процеси, методи пошуку, збору, зберігання, обробки, представлення, розповсюдження інформації та способи здійснення таких процесів і методів, є одними з найважливіших складових національних інтересів в інформаційній сфері .

Однак, поряд з перевагами побудови інформаційного суспільства, збільшуються і ризики, пов'язані з існуванням загроз безпеки інформаційним і телекомунікаційним засобам і системам. Захист інформаційних ресурсів від несанкціонованого доступу, знімання інформації засобами технічних розвідок, забезпечення безпеки інформаційних і телекомунікаційних систем, також є одним з основних національних інтересів в інформаційній сфері .

У зв'язку з цим виникає необхідність розробки сучасних методів і систем захисту інформації від різних типів загроз у всіх перерахованих системах.

Досить велика кількість засобів і систем захисту інформації створюються на основі математичних моделей, з використанням методів цифрової обробки сигналів а також використовують у своїй роботі інтенсивні логічні обчислення. До таких пристроїв відносяться технічні та криптографічні засоби захисту інформації, засоби захисту від помилок, системи розмежування доступу, а також процеси моделювання засобів та систем захисту інформації.

Для забезпечення безпеки інформації, при її обробки в інформаційних системах, розробляють і використовують політику безпеки, під якою розуміється сукупність норм і правил,що регламентують процес обробки інформації, виконання яких забезпечує захист від певної множини загроз і становить необхідну (а іноді і достатню) умову безпеки системи. Формальний вираз політики безпеки називається моделлю політики безпеки. Основні моделі політик безпеки можуть бути наступні: дискреціонна, мандатна, рольова, безпеки інформаційних потоків, ізольованої програмного середовища. В дискреціонній моделі розмежування доступу основою є матриця доступу, визначальна наявність того чи іншого права суб'єкта по відношенню до об'єкта інформаційної системи. Визначення прав в відповідності з матрицею доступу можна звести до обрахунку системи булевих функцій. Політика рольового розмежування доступу є розвитком політики дискреційного розмежування доступу, при цьому права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх застосування, утворюючи ролі.

В даний час розроблено цілий ряд методів захисту інформації в інформаційних системах, для реалізації яких існує безліч засобів захисту, що постійно оновлюються. Кожна конкретна захищена інформаційна система має свої особливості (важливість оброблюваної і збереженої інформації, умови функціонування і т. п.), які визначають вимоги до системи захисту інформації. У цих умовах практично важливим є отримання оцінок ефективності різних варіантів реалізації системи захисту інформації, що згодом може бути використано для вибору оптимального з точки зору пропонованих вимог комплексу захисних методів і засобів, необхідних для її створення .

Список використаних джерел:

3. Довбня С.Я., Нікірін А.В., Четверіков І.О. Методичні підходи щодо організації захисту інформації та раціонального вибору технічних засобів інформації// Бізнес і безпека. — 2013. — №6. — С . 78–80., Бізнес і безпека. — 2014. — №1. — С . 71–72.

УДК 621.39

Довбня С.Я. к.в.н., доцент, Кошиченко А.В., Нікірін А.В. к.т.н, Седько В.О.,
Київський національний університет імені Тараса Шевченка, andreyko2407@meta.ua

АНАЛІЗ ВИКОРИСТАННЯ УЗГОДЖЕНИХ СИГНАЛІВ ПРИ ПРОЕКТУВАННІ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ З БЕЗПІЛОТНИМИ ЛЕТАЛЬНИМИ АПАРАТАМИ

В даний час одним з актуальних питань є проектування захищеної інформаційно-телекомунікаційної системи (далі ЗІТС) з безпілотним літальним апаратом (БПЛА), що вимагає комплексного підходу до проектування планера, бортових інформаційних систем, системі автоматичного управління, каналу зв'язку та наземного обладнання [1,2].

Це викликано, з одного боку, розширенням сфери застосування, а з іншого — підвищенням вимог до передачі отриманої БПЛА інформації і як наслідок, підвищенням вимог до її безпеки та збереження.

Забезпечення роботи безпілотного комплексу повністю залежить від можливості стабільної і продуктивної комплексної обробки інформації, що надходить на різні датчики і системи. Часткове або повне вимкнення людини з каналів управління, перекладає відповідальність за прийняття рішення в реальному часі на бортові системи. У зв'язку з цим інформації на борту при обмежених ресурсах повинно бути якомога більше, і вона повинна бути прийнятою та обробленої якомога швидше і надійніше.

Зміна енергетичного запасу в каналі зв'язку дозволяє створити адаптивну радіотехнічну систему, здатну максимально ефективно використовувати енергетичний ресурс за допомогою адаптивної зміни параметрів цифрових систем зв'язку. Одним з основних адаптивно змінюваних параметрів є вид модуляції. Для підтримки на заданому рівні значення ймовірності бітової помилки, при різному відношенні сигнал/шум (ВСШ) на вході приймача, необхідно адоптивно змінювати порядок модуляції. При малих відстанях між ЛА та НКУ необхідно використовувати види модуляції з низькою енергетичною і високої спектральної ефективністю. Зі збільшенням відстані і при зниженні ВСШ слід перемикатися на енергетично більш ефективні і види модуляції. Визначення ВСШ може бути визначені за даними про кількість помилок канального декодера.

В якості адаптивно змінюваних параметрів системи зв'язку пропонується використовувати комплекс характеристик: вид модуляції, характеристики канального кодування, смугу пропускання системи, швидкість передачі даних, вихідну потужність передавача, співвідношення часу роботи на прийом і на передачу для напівдуплексних каналів зв'язку та ін. Реалізація адаптивної зміни співвідношення часу роботи на прийом і на передачу дозволить при високій швидкості передачі даних виділяти велику частину часу на передачу даних з борту Л на НКУ та приводити це співвідношення до одиниці, коли система працює на межі своїх можливостей і передає тільки командно — телеметричні дані.

В процесі виконання льотного завдання взаємне положення літального апарату (ЛА) та НКУ постійно змінюється, як наслідок — змінюються умови проходження сигналу на трасі.

Реалізація незалежних систем передачі даних для кожного каналу не завжди виправдана в силу підвищення вартості зв'язкового обладнання, а також збільшення його маси і габаритів. Крім того, в деяких випадках є необхідність передачі даних від великого числа незалежних джерел інформації, і реалізація окремих систем зв'язку для кожного каналу стає неможливою. Виникає проблема створення єдиної багатоканальної системи зв'язку з можливістю перерозподілу енергетичної ефективності між окремими каналами зв'язку. Один з підходів вирішення даної проблеми передбачає використання модифікованих сигнальних сузір'їв.

Список використаних джерел:

1. Игнатьев О. БЛА: Состояние и перспективы их использования в интересах НАТО. «Зарубежное Военное Обозрение». — 2010. — №12. — С. 45-52.

2. Слюсар В. Передача данных с борта БПЛА: стандарты НАТО. — ЭЛЕКТРОНИКА: НТБ, 2010, № 3, с. 80–86.

УДК 681.3.06

С.П. Евсеев, к.т.н., Т.А. Свердло

Харьковский национальный экономический університет им. Семена Кузнеца, Харьков,

evseev_serg@inbox.ru, tamara.sverdlo@hneu.net

МЕХАНИЗМЫ ИНТЕГРИРОВАННОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ДОСТОВЕРНОСТИ ДАННЫХ НА ОСНОВЕ КРИПТО-КОДОВЫХ СИСТЕМ

Защита компьютерных сетей и систем от несанкционированного доступа в современных условиях приобрела особую остроту. Развитие коммуникационных технологий позволяет строить сети распределенной архитектуры, объединяющие большое количество сегментов, расположенных на значительном удалении друг от друга. Все это вызывает увеличение числа узлов сетей и количества различных линий связи между ними, что, повышает риск несанкционированного подключения к сети и доступа к важной информации. Увеличение объемов обрабатываемых и передаваемых данных в компьютерных системах и сетях требует новых подходов в организации протоколов и механизмов обеспечения безопасности передаваемых данных. Отказ системы или выход за установленные ограничения указанных параметров может привести к значительным финансовым и материальным потерям. Криптографические средства защиты информации должны обеспечивать своевременную обработку огромных объемов данных (сотни Мбит/с) и удовлетворять жестким требованиям по достоверности и безопасности информации.

Механизмы обеспечения безопасности информации в компьютерных системах и сетях в большинстве основаны на криптографических методах — симметричной и несимметричной криптографии [1-4].

Известные несимметричные крипто-кодовые средства защиты информации строятся по двум схемам: с маскированием порождающей матрицы кода (схема Мак-Элиса) и с маскированием проверочной матрицы кода (схема Нидеррайтера) [1, 2]. Симметричная схема Рао-Нама по сути является некоторым упрощением несимметричной конструкции Мак-Элиса. В качестве исходных объектов могут выступать алгебраические блоковые коды с быстрым алгоритмом декодирования, такие, например, как коды Гоппы, Рида-Соломона, Боуза-Чоудхури-Хоквигнема [1-4].

Наиболее эффективными по стойкости к алгоритмам криптоанализа являются крипто-кодовые средства защиты информации с недвоичными линейными блоковыми кодами, возникающими на алгебраических кривых — алгеброгеометрическими кодами [4]. С одной стороны, подобные конструкции устойчивы к атакам, предложенным Сидельниковым [3], с другой стороны, они обеспечивают высокие показатели достоверности и оперативности передачи данных [4]. В тоже время практическое использование крипто-кодовых средств защиты информации с недвоичными алгебраическими блоковыми кодами предполагает применение методов и вычислительных алгоритмов недвоичного равновесного кодирования (по схемам Мак-Элиса и Ниддеррайтера).

Проведенный анализ показывает, что существующие нессиметричные криптографические средства защиты информации не обеспечивают современных требований: сложность реализации криптографических преобразований на 3-5 порядков выше, чем у аналогичных симметричных систем (блочно-симметричных шифров). Таким образом, в результате проведенных исследований выявлено объективно существующее противоречие между возрастанием объемов информации, которые подлежат несимметричному криптографическому преобразованию с обеспечением доказуемой стойкости, и лимитом времени для обработки информации криптографическими средствами защиты. Перспективным направлением дальнейших исследований является разработка и совершенствование крипто-кодовых средств защиты информации и протоколов обмена секретными сообщениями в различных режимах функционирования компьютерных систем и сетей.

Список використаних джерел:

1. McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory / R.J. McEliece // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January — February, 1978. — P. 114-116.

2. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory / H. Niederreiter // Probl. Control and Inform. Theory. — 1986. –V.15. — P. 19-34.

3. Сидельников В.М. Криптография и теория кодирования / В.М.Сидельников // Материалы конференции «Московский университет и развитие криптографии в России», МГУ. — 2002. — 22с.

4. Кузнецов А.А. Несимметричные криптосистемы доказуемой стойкости на алгебраических блоковых кодах / А.А. Кузнецов // Радіоелектронні і комп'ютерні системи. Науково-технічний журнал — Х.: ХАИ. — 2007.– №8(27) — С.130-144.

УДК 004.056.5

М.К. Жердєв, д.т.н.
І.В. Пампуха, к.т.н.
Г.Б. Жиров, к.т.н.
Військовий інститут Київського національного університету імені Тараса Шевченка

АЛГОРИТМ ШИФРУВАННЯ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ КЕРОВАНОГО, ВИПАДКОВОГО ТА НЕЛІНІЙНОГО ЕЛЕМЕНТА ГЕНЕРАЦІЇ КЛЮЧІВ

При широкому використанні сучасних телекомунікаційних систем, питання безпеки та захисту інформації від несанкціонованого доступу виходять на перший план.

Стрімке поширення комп'ютерних систем та їх взаємодія в мережах створило велику залежність користувачів від комп'ютерних вірусів, хакерів, електронного підслуховування, шахрайства і т.д. Захист інформації, яка пересилається по мережі і зберігається в таких системах, стала однією з найважливіших проблем сучасності. Відповідно до цього, виникає задача розробки алгоритму криптографічного перетворення інформації з випадковими ключами на нових перспективних підходах, у якого були б усунені недоліки існуючих алгоритмів.

В основу розробленого алгоритму криптографічного перетворення з випадковими ключами покладена ідея Вернама, в якій він запропонував відмовитися від детермінованих ключів, а генерувати ключ випадковим чином, при цьому довжина ключа повинна дорівнювати довжині повідомлення. Така схема отримала назву стрічки одноразового використання. В результаті застосування даної схеми на виході виходить випадкова послідовність, яка не має статистичного взаємозв'язку з відкритим текстом. Таким чином, в даному випадку, шифрований текст не дає ніякої інформації про сам текст, і отже не існує способу зламати такий ключ.

Складність практичного застосування цього алгоритму полягає в тому, що відправник і одержувач повинні мати один і той самий випадковий ключ.

Авторам розробленого алгоритму вдалося забезпечити синхронну і синфазну роботу генераторів випадкових чисел на передавальній та приймальній сторонах, при цьому відправник і одержувач мають один і той самий випадковий ключ. В алгоритмі використовуються як симетричні випадкові так і особисті ключі. Математично доведено, що визначити їх практично неможливо. Використання таких ключів та хеш-функцій дозволяє

вирішувати ряд додаткових завдань, а саме: захист мереж і терміналів від несанкціонованого доступу, аутентифікація, електронний підпис та ін.

Алгоритм може бути реалізований як програмно, так і програмно-апаратно, а також він задовольняє криптографічним вимогам, і за своїми можливостями може бути використаний для захисту конфіденційної інформації.

Принцип роботи алгоритму розглянемо на простому прикладі захисту мереж і терміналів від несанкціонованого доступу для двох абонентів, що реалізовано у пристрої ПЗМТ-1.

Структурна схема реалізації алгоритму АСК — 59140А — 06 для двох абонентів при обміні даних представлена на рис. 1. Відкриті (незашифровані) дані з виходу ЕОМ надходять на пристрій ПЗМТ-1, де шифруються, і вже «закриті» дані надходять на модем, в якому перетворюються і подаються в лінію зв'язку. По лінії зв'язку зашифровані дані через АТС та ін. елементи надходять на модем приймальної частини. З виходу модему ЗД подаються на ПЗМТ-1, де дешифруються і передаються на ЕОМ споживача.

Рис. 1. Структурна схема включення ПЗМТ-1 у мережу обміну даними між двома абонентами

Виходячи з структурної схеми видно, що ПЗМТ-1 включений в мережу послідовно з ЕОМ, і відповідно виконує функцію фільтру інформації. Якщо ця інформація не відповідає ключу, то вона руйнується на виході ПЗМТ-1. Таким чином, пристрій захищає не тільки інформацію в мережі, але і ЕОМ, як від атак вірусів, так і від несанкціонованого доступу до неї через дану мережу.

Структурна схема організації обміну між абонентами наведена на рис. 2. На етапі виробництва, при програмуванні пристрою ПЗМТ-1, пам'ять якого надійно захищена від несанкціонованого доступу, абонентам попарно присвоюються особисті і випадкові ключі.

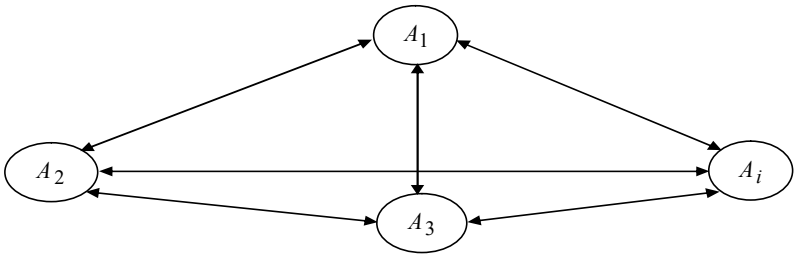


Рис. 2. Структурная схема организации обмена между абонентами

Наприклад, для абонентів $\grave{A}_1$ та $\grave{A}_2$ присвоюється ключ $K_{12} = K_{21}$. Для мережі (рис. 2), принцип побудови ключів наведено в табл. 1.

Таблица 1.

A_i / A_j	A_1	A_2	A_3	...	A_j
A_1		K_{12}	K_{13}	...	K_{1j}
A_2	K_{21}		K_{23}	...	K_{2j}
A_3	K_{31}	K_{32}		...	K_{3j}
...	...	...	...		...
A_i	K_{i1}	K_{i2}	K_{i3}	...	

Криптографічне перетворення в алгоритмі АСК — 59140А — 06 здійснюється по блоках, розмір якого становить 128 біт.

Таким чином, розроблений і запропонований алгоритм криптографічного перетворення, що володіє наступними характеристиками:

1. Ключі симетричні. Формуються випадковим чином, нікому не призначаються і не розподіляються, є особистими, випадковими і єдиними на множині 2^n (де n — число розрядів в блоці, що оброблюється) в процесі обміну інформацією між двома абонентами. При цьому їх довжина порівнянна з довжиною переданих повідомлень.

2. При реалізації алгоритму забезпечується:

- автоматичний контроль обміну інформацією між абонентами;

- високий ступінь криптографічного захисту інформації з еквівалентною довжиною ключа $K = 2^{3n}$ на один блок інформації;

- висока надійність передачі інформації, так як вона опосередковано пакетно порівнюється на приймальній та передавальній сторонах за допомогою хеш-функції.

При цьому, розроблений алгоритм може бути застосований в таких областях, як: телефонні мережі і факси, мобільні телефони, системи радіолокаційного розпізнавання літальних об'єктів, супутникові системи зв'язку, системи охоронної сигналізації, системи супутникової охорони та спостереження за об'єктами, захист банківських рахунків і операцій в банкоматах, захист інформації на електронних носіях, захист глобальної мережі Інтернет, захист корпоративних мереж шляхом аналізу вхідного потоку інформації.

Список використаних джерел:

1. Пат.88455 Украина, Спосіб зашифрування-розшифрування цифрової інформації з використанням керованого, випадкового, нелінійного і адаптивного елемента / заявник та патентовласник Всеукр. наук.–дослідн. ін-т зв’язку; заявл. 26.10.09.

УДК 004.056.53

Т.С. Запорожець

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут»

championka000@gmail.com

ФУНКЦІОНАЛЬНА МОДЕЛЬ БАЗИ ДАНИХ ЗАГРОЗ БЕЗПЕЦІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Державні інформаційні ресурси являють собою певну цінність, мають відповідне матеріальне вираження та вимагають захисту від різноманітних за своєю сутністю впливів. Впливи, які призводять до зниження їх цінності називаються несприятливими та тлумачаться як загрози. Тому для унеможливлення реалізації загроз розробляється та впроваджується комплексна система захисту інформації. Побудова такої системи передбачає визначення потенційних загроз та їх представлення відповідною моделлю. Для формування такої моделі пропонується розробити базу даних загроз безпеці державних інформаційних ресурсів.

Проектування означеної бази даних здійснюється на трьох рівнях: концептуальному, логічному та фізичному. Зокрема, на концептуальному рівні визначається, наприклад, мета побудови бази даних, основні функції, форми представлення даних і вимоги користувачів. Виконання цього переліку завдань здійснено шляхом функціонального моделювання бази даних загроз безпеці державних інформаційних ресурсів в нотації IDEF0. Такий підхід дозволяє здійснити її графічне описання, сформулювати мету та точку зору побудови. Графічний опис відображає базу даних через функцію або набір функцій, що визначають її можливості. Тоді як метою та точкою зору побуди бази даних встановлюється призначення та для кого вона створюється.

Функціональна модель бази даних загроз безпеці державних інформаційних ресурсів в графічній нотації IDEF0 представляється контекстною діаграмою як поєднання відповідних блоків та стрілок зі сформульованими метою та точкою зору. Блок контекстної діаграми є основним її компонентом та моделює означену базу даних. Стрілками позначаються дані або матеріальні об'єкти, що необхідні для формулювання моделі загроз. Так, на вхід блоку подаються реєстраційні дані, дані авторизації та інформація, що вноситься до бази даних. На виході блоку отримуємо модель загроз безпеці державних інформаційних ресурсів з урахуванням позначених стрілками вимог (обмежень) та ресурсів.

Таким чином, за результатами функціонального моделювання формалізовано використання бази даних загроз безпеці державних інформаційних ресурсів. Зокрема, визначено її призначення, мету та точку зору використання, а також можливості шляхом побудови функціональної моделі.

Означену модель буде використано для створення логічної та фізичної моделей на етапі даталогічного проектування бази даних загроз безпеці державних інформаційних ресурсів.

Науковий керівник — к.т.н. В.В. Цуркан

UDC 53.01

Zhivkov A.P., Frolov A.V.
PTI, NTUU"KPI", Kiev, Ukraine
zhivkov@yandex.ua

THE MYSTERIOUS NUMBER 137 OF QED AND MODERN DAY MEANS OF INFORMATION SECURITY

With the development of nanotechnology and perspectives of creating electronic schemes of information storing and processing to be based on graphene, researches are more often encountering the mysterious constant of the micro world — the fine structure constant α.

It appeared at first in Sommerfeld's research on the effect of splitting of spectral lines into several components in the presence of a static magnetic field (Zeeman effect) [1]. Zeeman notes that $\alpha = 1/137$ is "a constant and possibly a value, inversed to an integer".

For the second time the fine structure constant and external magnetic field became the subject of a close study by physicists after discovery of the quantum Hall effect. A new constant found it's usage among the scientific circles — the resistance quantum, given by the von Klitzing constant $R_K = h/e^2$ and related in the International System of Units to the fine structure constant as $R_K = Z_0/2\alpha$.

In this report, authors note that in M. Born's famous work where "electronic units of energy and length" are used (which stand for energy and radius of electron's orbit in terms used by Born, unlike so called atomic units, considered in the same work) [2], the term $1/2\alpha$ is the value of Bohr magneton.

Chronologically, the next appearance of fine structure constant was in the role of connection constant in famous Feynman diagrams, which are still used today.

In 2008, researchers, familiar to the "character" of fine structure constant, were not surprised (although, failed to explain up to the day) to found that the constant reappeared in "soft" light reflection coefficient from graphene $\Gamma = \alpha\pi$.

Being conducted at the Department of Technical Means of Information Security of PTI for a few years already, researches on the nature of fine structure constant have divided themselves into two complementary directions, in which the researched on constant is considered both as a constant and as a value, inversed to integer 137. [3]

In this report, considered are:

- numerical properties of the constant as of the norm of Gaussian integer $11+i4$;
- the possibility of representing it as a quaternion;
- the interconnection of these numerical representations with geometrical representations [4];

The importance of this consideration is determined by the fact that before the "physical" quantum Hall effect was found, mathematicians have already solved the corresponding topological problem. [4]

References

A. Sommerfeld, Atombau und Spektrallinien, Braunschweig: F. Vieweg & Sohn, 1921.

M. Born, "The Mysterious Number 137," in *Proceedings of the Indian Academy of Sciences — Section A* , Bangalore, 1935.

A. Zhivkov, E. Machusky and A. Frolov, "ON SOME NUMERICAL PROPERTIES OF THE FINE STRUCTURE CONSTANT," in *Третя міжнародна науково-практична конференція «Математика в сучасному технічному університеті»*, Kiev, 2015.

В. Арнольд, Геометрия комплексных чисел, кватернионов и спинов, Москва: Издательство Московского Центра Непрерывного Математического Образования, 2002.

UDC 53.01

E.A.Machusky, prof., D.Sc.

National Technical University of Ukraine "Kyiv Polytechnic Institute", sivera@ukr.net

STAIRSING OF 137 PRIME AS A STAR SING OF NATURE

Some "secrets" of number 137 are well known (en.wiki.prime 137 curious):

$$Integer[\pi \cdot 10^6] = 3141592 = 3^2 + 1^2 + 4^2 + 1^2 + 5^2 + 9^2 + 2^2 = 9 + 1 + 16 + 1 + 25 + 81 + 4 = 137$$

$$123456787654321 = 11^2 \cdot 73^2 \cdot 101^2 \cdot 137^2$$

Some more "secrets" are discovered by author:

$$\sqrt{\pi^2 + 137^2} \approx 137.036 + (\pi/2) \cdot 10^{-5}.$$

$$Integer[e \cdot 10^{10}] = 27182818284 = 137 \cdot 12 \cdot 16534561.$$

Median of $[\pi, e]$ is

$$(\sqrt{(\pi^2 + e^2)/2} + (\pi + e)/2 + \sqrt{\pi \cdot e} + 2 \cdot \pi \cdot e/(\pi + e))/4 \approx 2.9261098 + 1618 \cdot 10^{-11},$$

where $1618/10^3$ is "golden ratio".

$$(\pi \cdot e/100)^2 \approx 0.0072927...$$

$$1/137 \approx 0.007299270072992700727927...$$

$$1/137 = 729927/10^8 + 729927/10^{16} + 729927/10^{24}...$$

$$1/137 = (10^8 - 1)/10^8 + (10^8 - 1)/10^{16} + (10^8 - 1)/10^{24}...$$

$$1/137 = 99999999/100000000 + 99999999/10000000000000000 + ...$$

But the main secrets of 137 number are the next:

Alpha stairsing

$$1^3 = 1$$
$$11^3 = 1331$$
$$111^3 = 1367631$$
$$1111^3 = 1371330631$$
$$11111^3 = 1371700960631$$
$$111111^3 = 1371737997260631$$
$$1111111^3 = 1371741700960260631$$
$$11111111^3 = 1371742071330590260631$$
$$111111111^3 = 1371742108367626890260631$$
$$1111111111^3 = 1371742112071330589890260631$$
$$11111111111^3 = 1371742112441700060219890260631$$
$$111111111111^3 = 1371742112478737997256519890260631$$
$$(111\ 111\ 111\ 111\ 111\ 111\ 111\ 111...)^3 = 137\ 174\ 211\ 248\ 285\ 322\ 359...$$
$$(11.1111111111...)^3 = 137 + (137 + 1 \cdot (137 - 100))/10^5 + (137 + 2 \cdot (137 - 100))/10^8 + \\ + (137 + 3 \cdot (137 - 100))/10^{11} + ...$$

and as a result

$$(10/9)^3 = 1000/729 = 10^3/3^6 = \sum_{n=0}^{\infty} (137 \cdot (n+1) - 100 \cdot n)/10^{3\cdot(n+1)-1} .$$

Mysterious number 137 is simply the connection constant of the positional calculation systems.

Actually it is a star sing of nature!

УДК 004.773

В.О. Міщенко

Навчально-науковий центр підвищення кваліфікації, перепідготовки і дистанційного навчання Державного університету телекомунікацій

О.В. Драглюк

Науковий центр зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації Державного університету телекомунікацій

СТВОРЕННЯ ЗАХИЩЕНОГО ОБМІНУ ГОЛОСОВОЮ ІНФОРМАЦІЄЮ З ДОПОМОГОЮ ТЕХНОЛОГІЙ VOIP ТА OPENVPN

Розвиток сучасних комп'ютерних технологій, використання інформаційних мереж відкриває колосальні можливості розвитку в усіх галузях освіти, науки, техніки та економіки. Прогрес в даній області вже давно вирішив проблему «останньої милі» та дозволяє користувачам мати доступ до глобальної мережі Інтернет та отримувати необхідну їм інформацію майже у будь якому місці планети та в реальному масштабі часу.

Знайшла своє розповсюдження й технологія передачі голосу через IP мережі — VoIP (Voice over IP), яка реалізує створення мереж обміну голосовою інформацією між користувачами та їх групами з використанням відповідного

програмного та апаратного забезпечення, що використовує технологію клієнт-сервер. На даному етапі розвитку програмні засоби VoIP уже мають можливість бути встановленими в кінцеві пристрої користувачів такі як: смартфони, планшетні ПК, ноутбуки, ПЕОМ, тощо. Вони не потребують значних ресурсів та пропускних спроможностей мереж зв'язку. Одним з напрямів даної технології, який набув розвитку в останні роки є так-звані push-to-talk додатки. До найпоширеніших програмних агентів, що використовуються, належать Zello, TeamSpeak та ін.

Проте відсутність в даних додатках засобів захисту та шифрування повідомлень не дозволяють використовувати їх безпечно.

Для вирішення даної проблеми пропонується використовувати програмні засоби, які дозволяють створювати VPN з'єднання.

На сучасному ринку присутня досить велика кількість програмних додатків даного типу, більшість з яких пропрієтарні. Серед безкоштовних засобів найбільшою популярністю користується програмний засіб OpenVPN. Слід відмітити, що даний додаток має програмні реалізації для всіх сучасних операційних систем, невимогливий до ресурсів та зручний у користуванні. Крім того, перевагою даного продукту є можливість використання від 128 до 2048 бітних ключів шифрування, налаштування додаткових політик безпеки для авторизації користувачів.

Впровадження сукупності даних технологій дозволяє:

використовувати кінцеві пристрої користувачів: смартфони, планшетні ПК, ноутбуки, ПЕОМ;

використовувати будь-які сучасні стандарти передачі даних;

створювати захищені канали зв'язку між абонентами з ключами шифрування до 2048 біт;

мати постійно діючу захищену систему обміну голосовими повідомленнями;

не витрачати додаткові коштів на впровадження.

УДК 004.056.53+621.391.814

Морозова А.Д.

ХНУРЭ, ancho.morozova.94@bk.ru

ИССЛЕДОВАНИЕ МЕТОДА ВЧ-НАВЯЗЫВАНИЯ В ТЕЛЕФОННОЙ ЛИНИИ

В настоящее время защитой распространённого и достаточно уязвимого канала передачи информации — телефонной линии — почему-то пренебрегают. Отметим, что проводная телефонная сеть является одной из самых распространённых средств связи и, несмотря на развитие беспроводных технологий передачи информации, многие организации не отказываются от использования телефонных линий связи. Её наличие на территории объекта представляет собой угрозу для информационной безопасности. Кроме перехвата самих телефонных разговоров у злоумышленника есть возможность

перехвата акустической информации при положенной трубке телефонного аппарата методом ВЧ-навязывания.

АЧХ телефонной линии с подключенным эквивалентом телефонного аппарата (рис.1) при реализации метода ВЧ-навязывания для различной длины линии показано на рис.2.

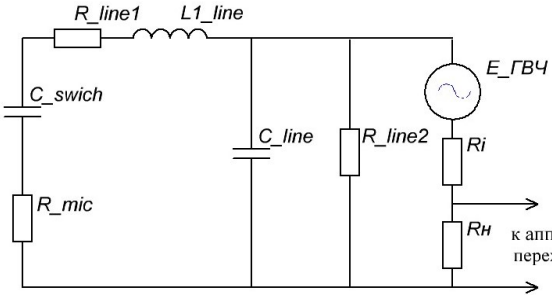


Рисунок 1 — Эквивалентная схема несанкционированного съёма информации методом ВЧ-навязывания

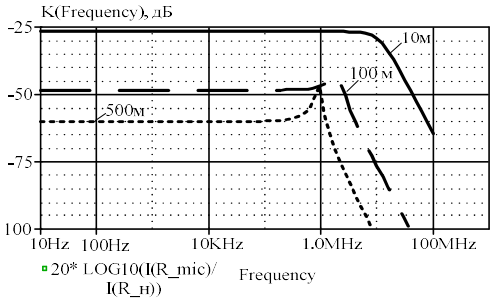


Рисунок 2 — АЧХ телефонной линии (при её различных длинах) с учётом эквивалента телефонного аппарата при реализации метода ВЧ-навязывания

При этом комплексная передаточная функция описывается следующим выражением:

$$K(jf) = \frac{R_н}{R_i + R_н + \dfrac{\left(R_{mic} + \dfrac{1}{j\omega C_{swic}} + R_{line1} + j\omega L1_{line}\right)\dfrac{\dfrac{1}{j\omega C_{line}} R_{line}}{\dfrac{1}{j\omega C_{line}} + R_{lin}}}{R_{mic} + \dfrac{1}{j\omega C_{swic}} + R_{line1} + j\omega L1_{line} + \dfrac{\dfrac{1}{j\omega C_{line}} R_{line}}{\dfrac{1}{j\omega C_{line}} + R_{lin}}}} \quad (1)$$

В зависимости от длины телефонной линии граничная частота генератора ВЧ-навязывания может находиться в пределах 1…10 МГц.

В роботе исследована возможность применения метода к электронным телефонным аппаратам и выявлено, что большая вероятность утечки информации, например, с ТА-72 обусловлена наличием резонанса, созданного обмоткой дифференциального трансформатора и паразитной ёмкостью рычажного переключателя. В некоторых моделях телефонных аппаратах минимальное ослабление составляет 80 дБ, поэтому вероятность утечки информации в них, даже без применения защитных фильтров — минимальна.

Полученные в работе результаты позволяют более эффективно обеспечить защиту телефонной линии от несанкционированного съема информации методом ВЧ-навязывания.

Научный руководитель — к.т.н., доц. Ю.В. Лыков

УДК 004.056:534.6 **С.М. Нужний, к.т.н.**
Національного університету кораблебудування ім. адм. Макарова, м. Миколаїв
s.nuzhniy@gmail.com

НОВІ НАПРЯМКИ В ЗАБЕЗПЕЧЕННІ ЗАХИЩЕНОСТІ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Найбільш ефективним методом протидії витоку акустичної (мовної) інформації в наш час є використання активних методів зашумлення. Їх основою є генератори завади. До недавнішнього часу вони будувались на основі генераторів «білого шуму» та/чи його модифікацій — так званих «кольорових шумів». Однак розвиток спеціалізованих напрямків аналізу складних сигналів та принципів формування мовних сигналів дозволили створити методики, які дозволяють проводити очищення фонограм сигналів від такого типу шумів.

Як додаткову опцію для типових генераторів «білого шуму», останнім часом, в багатьох випадках виробники пристроїв для постановки перешкод, почали додавати режим генерування мовоподібної перешкоди.

Аналіз застосування таких перешкод показує їх значний потенціал, однак є декілька перепон, що дещо дезорієнтують користувачів таких систем, і є характерними для початкового етапу розвитку будь-якої нової техніки та технологій. Головними з таких перепон є жорстка вимога нормативних документів до використання тільки систем, які побудовані на базі генераторів білого шуму. Тими ж нормативними документами регламентуються основні методики проведення перевірки захищеності інформації від витоку технічним (акустичним) каналом.

До перепон також необхідно віднести й деяку некоректність в тлумаченні самого терміну «мовоподібна перешкода», яка виникла в наслідок не відповідності прийнятих в середині 80-их років визначень сучасним можливостям наукових методів та технічних засобів. Так, під вказаним терміном в нормативних документах маються на увазі генератори перешкод, що побудовані на базі генераторів білого шуму, але мають нелінійну ЛАЧХ, яка оптимізована по енергетичному критерію до можливостей людського вуха та голосового апарату. Такий тип завади має деякі переваги над базовим варіантом перешкоди «білий шум» але, на сучасному етапі, не спроможний виправити їх системні недоліки.

Сучасний підхід в спеціалізованій літературі до вказаного терміну полягає в тому, що «мовоподібні» перешкоди формуються (синтезуються) з мовних сигналів. При цьому можливе формування перешкоди, як з мовних фрагментів (відрізків), які не корелюються з сигналом, який необхідно приховати, так і безпосередньо з нього.

Перешкоди, які формуються з мовних фрагментів, що не корелюються з сигналом, який необхідно приховувати, є перешкоди типу «мовної хор» або «гомін (галас) натовпу». Така перешкода формуються шляхом змішання фрагментів промови кількох людей (дикторів).

Серед «мовоподібних» перешкод, що формуються з сигналу, який необхідно приховувати, можна виділити два типи:

а) реверберaційну — перешкода формується з фрагментів приховуваного мовного сигналу шляхом багаторазового їх накладення з різними рівнями;

б) інверсійну − перешкода формується з приховуваного мовного сигналу шляхом складної інверсії його спектра.

Однак і такі пристрої мають ряд системних недоліків: обмеженість довжини коду формування завади (тобто він є псевдо випадковим) та можливість проведення зловмисником фільтрації несанкціонованих фонограм методами виявлення нетипових фонем

Запропоновано третій тип «мовоподібної» перешкоди, яка, в першому наближенні, може розглядатися як перешкода комбінованого типу, що має власну розширену систему криптографічного захисту, — «переставна». Перешкода формується з приховуваного мовного сигналу теперішнього та попереднього тактів, шляхом складного переставляння часових та частотних смуг з випадковими довжиною, кількістю та інверсією.

М.І. Рєзніков к.т.н, доцент, Д.О.Петрик, В.І.Семенюк
Київський національний університет імені Тараса Шевченка
Demendar@gmail.com

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ В МОБІЛЬНИХ МЕРЕЖАХ ТРЕТЬОГО ТА ЧЕТВЕРТОГО ПОКОЛІННЯ

В доповіді розглядаються методи захисту мереж 2 — 4-го покоління:

– шифровка переданих даних здійснювалася простим потоковим шифром, який на даний момент став доступний для взлому;

– авторизовані державою спецслужби повинні легко мати доступ до переданої інформації, але в GSM такі механізми не були враховані при створенні, і їх довелося добудовувати вже після затвердження стандарту;

– аутентифіковувався тільки користувач мережею, а не навпаки (зловмисник мав можливість вплинути на вироблення сесійного ключа і тим самим отримати доступ до інформації.

Проте, основні принципи політики безпеки GSM виправдали себе і лягли в основу механізмів захисту інформації UMTS (шифрування радіосигналу, використання модуля ідентифікації користувача, певна свобода вибору механізмів оператором і т.д.).

Захист інформації в UMTS

Перед початком обміну інформацією виконуються наступні процеси:

– взаємна аутентифікація;

– захист цілісності, угода про ключі цілісності між користувачем і обслуговуючою мережею;

– мережева безпека;

– безпеку сервісів і програм;

– взаємодія між мережами та роумінг.

Головним нововведенням є алгоритм аутентифікації та узгодження ключів, крім того у мережах UMTS, передбачено використання блочного

шифру f8 (1997р., Міцуру Мацуі), який володіє 128-бітовим ключем, 64-бітними блоками і варійованою кількістю ітерацій та перевірки цілісності за допомогою функції f9.

Захист інформації в LTE

Захист в мережі LTE передбачений на рівні доступу до мережі, на рівнях мережевого і користувацького доменів, на рівні програм та рівні відображення і конфігурацій. На кожному з цих рівнів:

- здійснюється аутентифікація всіх пристроїв;
- використання не тільки IP-адреси, а й системи розповсюдження ключів шифрування для всіх пристроїв, підключених до мережі;
- зберігаються методи аутентифікації користувачів по прив'язці до карти USIM.

У мережах LTE алгоритми шифрування і забезпечення комплексної безпеки засновані на технології Snow 3G і стандарті AES, в нових релізах планується використовуватися два додаткових алгоритми. Якщо один з алгоритмів буде зламаний, то інші, що залишилися повинні забезпечити безпеку мережі LTE.

Види загроз

Так як мережі UMTS та LTE направлені на комутацію пакетів, тобто використання протоколу IP, мережі вразливі до будь яких мережевих атак зі сторони зловмисників. Наприклад: DoS, DDoS, вірусні атаки (включаючи SSH), та атаки на сервіси.

Загроза користувачам LTE може виходити і від сервісів подвійного призначення, прикладом є LBS-сервіси.

Також загрозами для мережі є устаткування абонента (UE). Збільшується кількість телефонів з операційними системами, що мають ті самі можливості що і настільні комп’ютери тому потенційною проблемою є мобільні операційні системи, через які зловмисники можуть отримувати доступ як до устаткування абонента, так і до інформації, яка безпосередньо передається з базової станції або навпаки.

Слід зазначити що великою загрозою для мережі можуть бути фемто- та пікосоти, які встановлюються у приміщеннях для покращення покриття, які також можуть бути використанні зловмисниками.

Висновок:

Мережі UMTS та LTE є масовими стандартами бездротового зв'язку, що забезпечують високий рівень захисту інформації користувача у порівнянні з мережею GSM. Хоча мережі можуть бути атаковані зловмисниками, вони всеодно забезпечують достатній рівень захисту інформації відносно існуючих загроз.

Список використаної літератури:

1.3GPP Specifications, http://www.3gpp.org

2. Аналитический обзор защиты данных в сетях LTE По материалам NTT DOCOMO Technical Journal Vol. 11 No. 3

Г.М. Розорінов, проф., Н.А. Сидорков, студ., Н.І. Чичикало, проф.,

РАДІОЧАСТОТНА ІДЕНТИФІКАЦІЯ РУХЛИВИХ ОБ'ЄКТІВ СПЕЦІАЛІЗОВАНИХ ПРИМІЩЕНЬ

Радіочастотна ідентифікація (Radio Frequency Identification — RFID) — це технологія автоматичного безконтактного дистанційного виявлення, розпізнавання і оперативного супроводу, нерухомих і рухливих просторово розподілених об'єктів. Вона робить можливим швидке безконтактне прочитування інформації з невеликих радіоміток на відстані і за відсутності прямої видимості за допомогою стаціонарних і мобільних зчитувачів.

Інтегрована мікросхема мітки зберігає дані про об'єкт маркіровки і забезпечує необмежену кількість запису і прочитування. Швидкість роботи RFID досягає тисяч міток в секунду, тому система дозволяє одночасне прочитування великої кількості міток з промаркірованих об'єктів на ходу.

Дані в мітці можуть забезпечити ідентифікацію об'єкту на виробництві, товарів в магазині, на складі і при перевезенні, місцерозташування і ідентифікацію рухливих засобів, ідентифікацію тварин, людей, майна, документів та ін.

Система RFID складається з двох компонентів: мітки (тега, транспондера або безконтактного носія даних) і зчитувача (рідера). Основні компоненти системи радіочастотної ідентифікації : прочитуючий пристрій і транспондер.

Авторами була поставлена задача **р**озробити автоматизовану систему захисту об'єктів від несанкціонованого доступу методом радіочастотної идентифікації рухливих об'єктів спеціалізованих приміщень. З метою виключення шкідливого впливу постійно-діючих високих частот розробити електронні схеми транспондера і приймача/передавача на частотах в межах 8,21 кГц. Структурна схема розробки представлена на рис. 1.

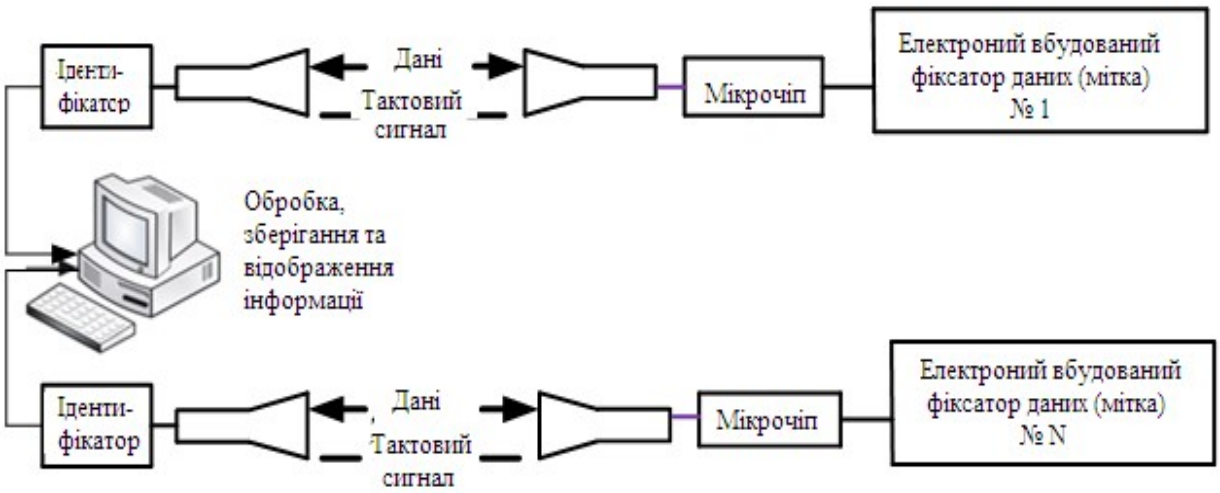


Рис.1. Основні компоненти системи радіочастотної ідентифікації: ідентифікатор-зчитуючий пристрій, електронний вбудований фіксатор — транспондер

Мітка складається з наступних основних компонентів: мікрочіпа і антени. Компоненти мікрочіпа включають: модулятор, логічну схему, виділник тактової частоти, кероване джерело живлення, пам'ять і приєднаний до антени. Антена вмонтована у відкритий контур індуктивного чутливого елементу, виконаного на спеціальному півсферичному феритовому сердечнику, включеному в схему генератора за схемою індуктивної трьохточки. Схема ідентифікатора — зчитувача включає приймачі/передавачі, мікропроцесор, що виконує функції кодера-декодера й алгоритм логічних операцій, інтерфейси введення/виводу і зв'язку. По частотному діапазону передбачаються низькочастотні мітки. Пристрої, що розробляються, придатні також для використання на промислових об'єктах особливої важливості.

Розорінов Г.М., проф., Фурса В.О., студ., Чичикало Н.І., проф.,

РОЗРОБКА ІНСТРУМЕНТУ ДЛЯ ЧАСТОТНО-ЧАСОВОГО АНАЛІЗУ СИГНАЛІВ В СЕРЕДОВИЩІ ГРАФІЧНОГО ПРОГРАМУВАННЯ LabVIEW

Перетворення Фур'є як метод аналізу сигналів неможливо застосувати на практиці, оскільки воно проектує сигнал на хвилі нескінченної довжини. Інші одновимірні концепції, такі як миттєва частота і групова затримка також не адаптовані до великого числа нестаціонарних сигналів, оскільки припускають відповідно монокомпонентность сигналу в одну мить і одинична поява однієї компоненти на інтервалі аналізу. Для аналізу складних нестаціонарних сигналів необхідно розглядати спільні частотно-часові розподіли.

Короткочасне перетворення Фур'є (КПФ). Щоб внести залежність за часом в КПФ, простим рішенням є виділення сигналу у вікні навколо моменту *t* і подальше обчислення КПФ для кожного моменту часу *t*. Таке перетворення КПФ описується як: $F_x(t,f;h)=\int_{-\infty}^{\infty} x(\tau)\cdot h^*(\tau-t)\cdot e^{-j2\pi f\tau}d\tau$, де $h(t)$ — короткочасне вікно аналізу. Перемножування з часовим вікном $h^*(\tau-t)$ ефективно пригнічує сигнал за межами деякої околиці моменту аналізу $t=\tau$., тобто КПФ — це локальний спектр сигналу *x(t)* навколо моменту τ. Квадратний модуль КПФ, — це спектральна щільність потужності сигналу, поміщеного у вікно $S_x(t,f)=\left|\int_{-\infty}^{\infty} x(\tau)\cdot h^*(\tau-t)\cdot e^{-j2\pi f\tau}d\tau\right|^2$. Це визначає спектрограму, як дійсний і ненегативний розподіл.

Частотно-часове перетворення Вігнера-Вілля визначається як:

$W_x(t,f)=\int_{-\infty}^{\infty} x(t+\tau/2)\cdot x^*(t-\tau/2)\cdot e^{-j2\pi f\tau}d\tau$. Воно задовольняє таким математичним властивостям як: збереження енергії, виконання маргінальних співвідношень, унітарність і інші, і є дійсно визначеним. Вимагає знання сигналу на нескінченному інтервалі, на практиці використовується $PW_x(t,f)=\int_{-\infty}^{\infty} h(\tau)\cdot x(t+\tau/2)\cdot x^*(t-\tau/2)\cdot e^{-j2\pi f\tau}d\tau$ — псевдорозподіл.

На рис. 1 показана фронтальна панель розробленої моделі приладу частотно-часового аналізу сигналів.

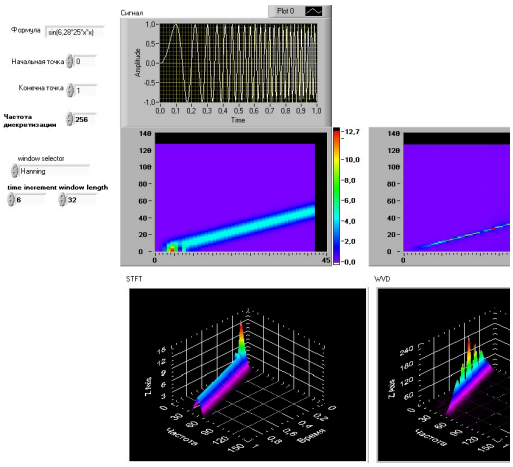


Рис. 1 Фронтальна панель розробленої моделі приладу

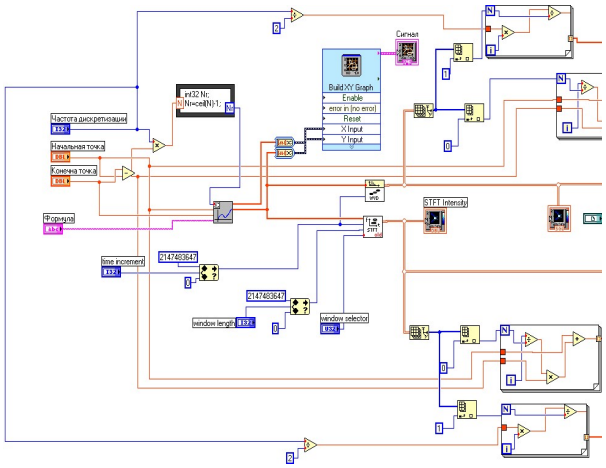
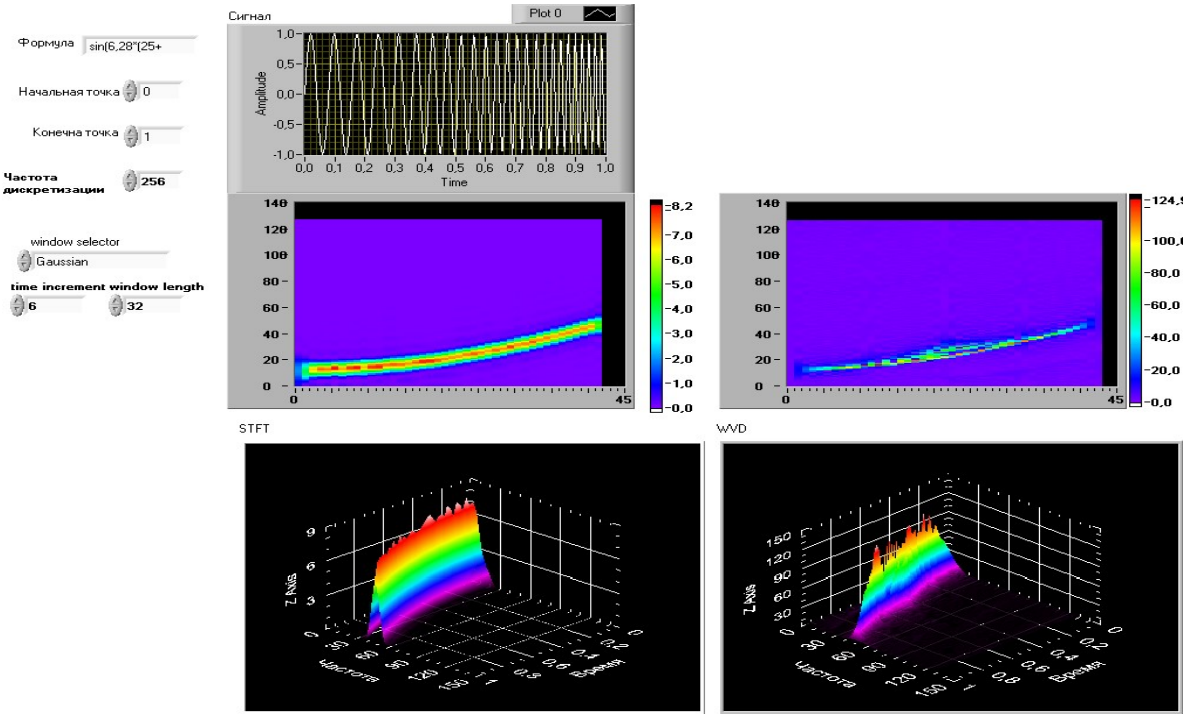


Рис. 2 Структурна схема розробленої моделі приладу

Панель містить елементи управління і індикації. До елементів управління відносяться: поле для завдання формули, що описує сигнал, поля для завдання початкового і кінцевого моменту моделювання сигналу і його частоти дискретизації, поле для вибору типу вікна, що зважує, при обчисленні спектрограми, а також його довжини; поле, де задається зрушення вікна, що зважує, в звітах при обчисленні спектрограми і розподілу Вігнера-Вілля. До елементів індикації відноситься вікно, де виводиться вид сигналу в часі, вікна, де виводиться спектрограма і розподіл Вігнера-Вілля у вигляді діаграми інтенсивностей і вікна, де вони виводяться у вигляді тривимірних графів. Структурна схема моделі приладу показана на рис. 2.

Результати роботи програми.

Для сигнала виду sin(6,28*(25+25*x*x)*x)



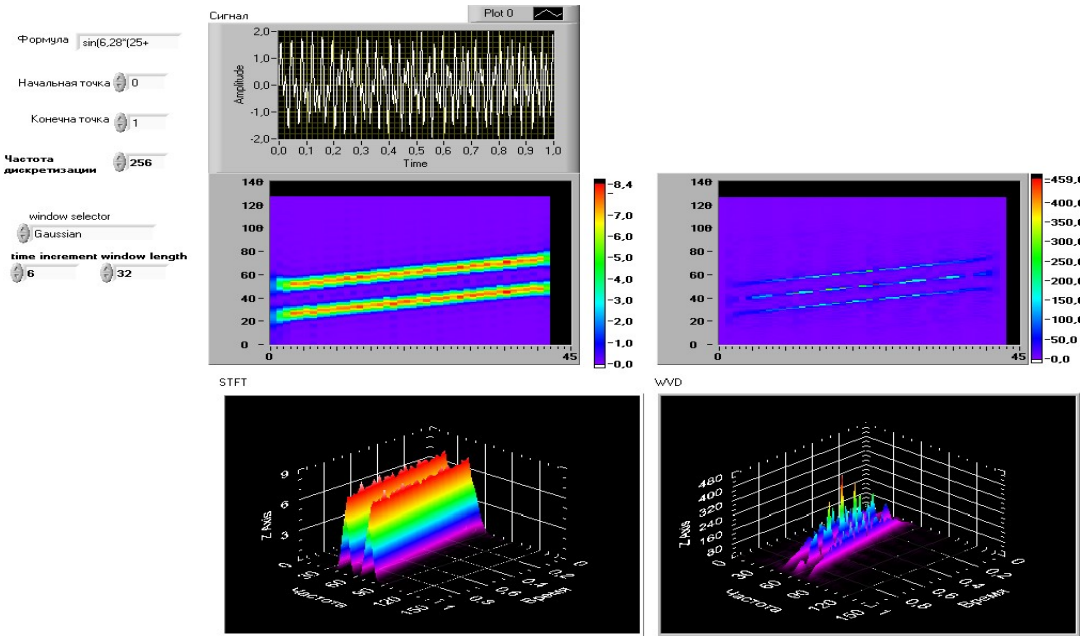
Для сигнала виду sin(6,28*(25+25*x)*x)+sin(6,28*(50+25*x)*x)

Висновки.

1. Розроблена модель приладу частотно-часового аналізу сигналів, що дозволяє розраховувати короткочасне перетворення Фур'є і перетворення Вігнера-Вілля, що виводить графіки в тривимірному уявленні та на граф інтенсивності.

2. Проведені дослідження характеристик отримуваних частотно-часових розподілів залежно від параметрів алгоритмів перетворення.

3. Тривимірні графи дозволяють переглядати частотно-часовий розподіл з різних ракурсів.



Розорінов Г.М., проф., Чичикало Н.І., проф., Бородін Д.Ю., студ.

РОЗРОБКА ВІРТУАЛЬНОГО ІНСТРУМЕНТУ «ПОШИРЕННЯ РАДІОХВИЛЬ» ДЛЯ ДОСЛІДЖЕННЯ РАДІОПЕРЕДАВАЛЬНОЇ СИСТЕМИ

В роботі запропонована структурна схема, яка дає можливість розрахунку відстані між приймальнею і передавальною антенами, ефективну площу приймальної антени, коефіцієнти корисної дії передавального і приймаючого трактів, а також потужність на вході приймача і дозволяє враховувати основні чинники і вплив зовнішнього середовища для використання в особливо складних виробничих умовах (рис. 1).

Математична модель досліджувальної системи має вигляд:

$$MOD_{РПКС} = \{\lambda = F(f); D = F(D_{дБ}); \eta_{пер} = F(A, K_{СВ});$$

$$A = F(\alpha, l); S_{эфф} = F(\lambda, D); P_{прм}^{\min} = F(P_{дБ/мВт}); P_{дБ/мВт} = F(P); \xi; \chi\},$$

де:

$$\lambda = 300/f;$$

$$D = 10^{D_{дБ}/10};$$

$$\eta_{пер} = A \cdot (1 - \Gamma^2) = A\left[1 - \left(\frac{КСВ - 1}{КСВ + 1}\right)^2\right];$$

$$A = 10^{\frac{\alpha l}{10}};$$

$$S_{эфф} = \frac{\lambda^2}{4\pi} \cdot D_{прА};\ P_{прм}^{\min} = 10^{\left(\frac{P(дБ/мВт)}{10} - 3\right)};$$

$$P[дБ/мВт] = 10lgP + 30.$$

ξ — коефіцієнт відбитку в металі; χ — коефіцієнт розсіювання.

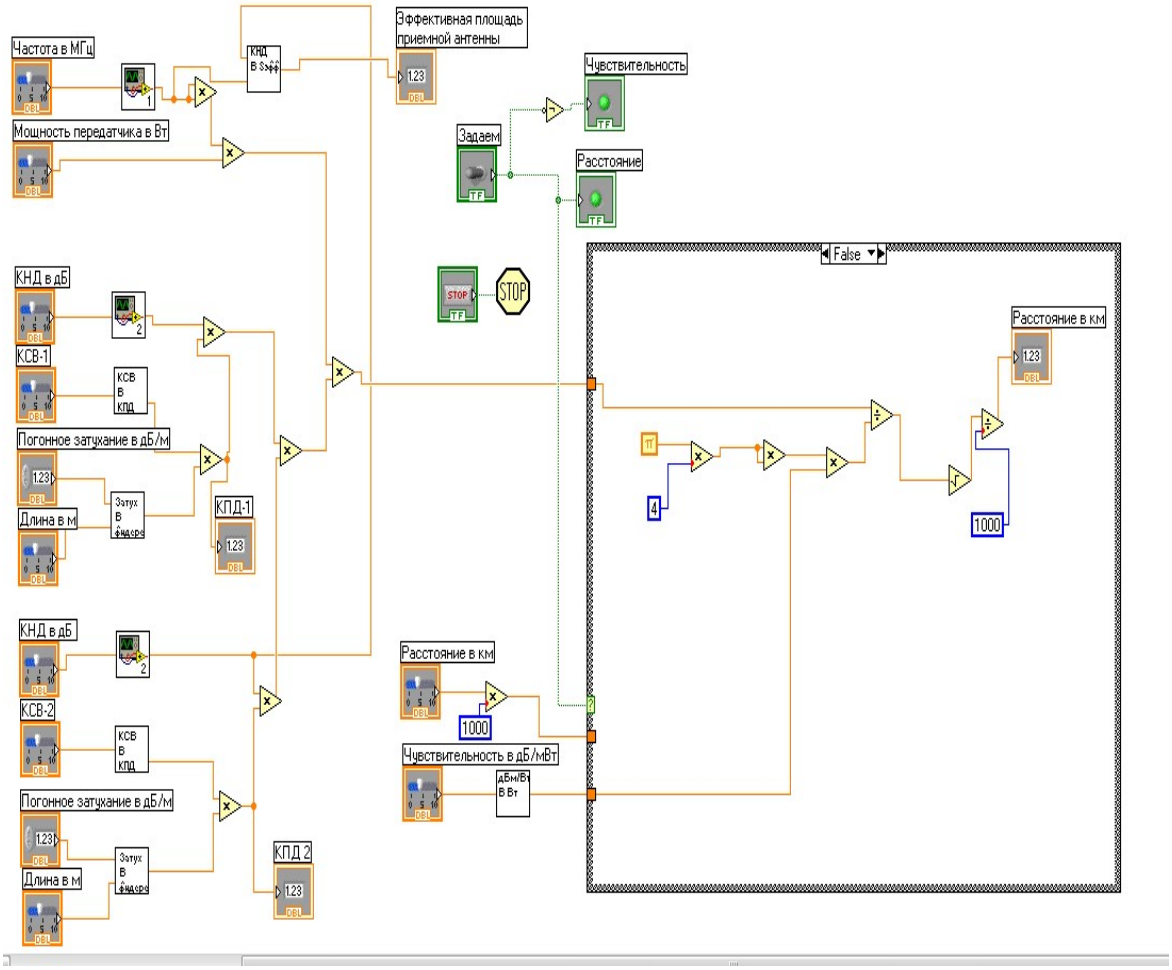


Рис. 1. Структурна схема для дослідження радіопередавальної системи

Висновки. Розроблена схема може бути використана для проектування радіопередавальних систем. Поширення радіохвилі з точки випромінювання в точку прийому відбувається в деякій істотній області простору. Проте їх вивчення у рамках натурного лабораторного експерименту вкрай ускладнене, зважаючи на сам масштаб цих явищ. В той же час цілком реально здійснити їх вивчення на математичних комп'ютерних моделях, наприклад з використанням засобів LabVIEW.

УДК 004.056.53

В.Ф. Свіжевський, студент; С.А. Зінченко, к.т.н., доцент
НТУУ «КПІ», Фізико-технічний інститут, grefendor@i.ua,ftzzi@pti.kpi.ua

ПАСИВНА АКУСТИЧНА СИСТЕМА ВИЯВЛЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Зі стрімким розвитком науки і техніки, компонентної бази, значно розширились можливі сфери застосування безпілотних літальних апаратів, які можуть використовуватись в громадських цілях, зокрема для спостереження, моніторингу радіаційної, хімічної, бактеріологічної обстановки та ін.

Актуальність роботи полягає в тому, що в теперішній час у вільному продажі з'явились безліч легкодоступних радіокерованих літальних моделей, з параметрами та характеристиками, які дозволяють їх використання в протиправних цілях, будь-якою зацікавленою особою.

Метою роботи є проведення аналізу щодо можливості виявлення малогабаритних безпілотних літальних апаратів (МБЛА) та точності встановлення їх координат в просторі.

Серед основних загроз, що можуть нести МБЛА слід виділити наступні: диверсійна діяльність (доставка вибухових, отруйних чи інших небезпечних речовин та пристроїв на об'єкт з метою нанесення шкоди персоналу, спорудам чи іншим технічним засобам, що там знаходяться; провокування хибного спрацювання систем захисту, встановлених на об'єкті); розвідувальна діяльність (фото та відео зйомка; хімічний, біологічний, радіаційний, акустичний, термічний та ін. моніторинг місцевості чи об'єкту); використання МБЛА в якості ретранслятора.

Сам пристрій виявлення МБЛА являє собою пасивний акустичний шумопеленгатор, в основі якого лежить система фазованих мікрофонних решіток, розташованих як дві лінійні еквідистантні решітки, перпендикулярні одна одній (хрест Мілса). Період таких решіток дорівнює 5см., що зумовлюється особливостями шуму, створюваного лопатями МБЛА. Прийомними елементами являються конденсаторні мікрофони, які мають діаграму спрямованості подібну до півсфери, та в без корпусному варіанті мають розміри 1-2 см. Для забезпечення ширини діаграми направленості однієї лінійної решітки 2°, а отже і точності встановлення координат, достатньо 24 елемента. В сумі одна хрестоподібна система буде містити 48 мікрофонних елементів, та мати габаритні розміри приблизно 140 на 140 см. Оскільки пристрій повинен виявляти МБЛА у всіх напрямках було вирішено розбити весь діапазон огляду на сектори, за кожен з яких буде відповідати окрема хрестоподібна система. Таке рішення значно повисить швидкодію системи виявлення за рахунок паралельної обробки сигналів на ЕОМ та дасть змогу в режимі реального часу будувати шумову обстановку простору. Описаний метод являється менш затратний ніж радіолокаційні методи, оскільки не містить дороговартісних компонент обробки сигналів на високих частотах. Може виявляти апарати, що не випромінюють сигнали в електромагнітному діапазоні.

Також, оскільки система пасивна, вона не містить демаскуючих факторів та не впливає на навколишнє середовище.

Для подальшого удосконалення представленої вище системи виявлення пропонується замінити конденсаторні мікрофони на п'єзокерамічні, які мають значно більшу чутливість. Для узгодження двох різних за жорсткістю середовищ слід використовувати перехідну ланку. Також для встановлення відстані до літального апарату можливо застосовувати систему двох спарених мікрофонних решіток, розташованих, наприклад, перпендикулярно одна одній.

Отже, в роботі була представлена ідея створення системи виявлення МБЛА. Були приведені оцінки основних параметрів системи. В подальшому планується впровадження адаптивних алгоритмів для захисту від завад та створення неперіодичних решіток для покращення виявлення МБЛА на малих відстанях.

Науковий керівник — кандидат технічних наук, доцент С.А. Зінченко.

УДК 004.056

М.В. Турти

Національний університет кораблебудування імені адмірала Макарова, turtym@meta.ua

ПРИНЦИПИ ВИБОРУ МЕТОДУ ФОРМУВАННЯ ФУНКЦІЙ НАЛЕЖНОСТІ ДЛЯ ЗАДАЧ ОБРОБКИ НЕЧІТКИХ ДАНИХ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Вступ. В багатьох системах технічного захисту інформації передбачається розпізнавання об'єктів, процесів та ситуацій на основі нечітких даних. Первинною задачею при побудові таких систем є формування функцій належності (ФН) досліджуваних об'єктів та нечітких еталонів, що можуть бути представлені в різних формах. На даний час існують різноманітні методи побудови ФН [1, 2], що характеризуються особливостями алгоритмів отримання та обробки експертних даних і здатні формувати ФН з певними властивостями, однак рекомендації щодо вибору методу формування ФН для певних прикладних задач наявні тільки для окремих методів і не мають систематизованого характеру [3-5].

Метою даної роботи є визначення принципів вибору методу формування функцій належності для прикладних задач інформаційної безпеки (ІБ).

Для досягнення поставленої мети необхідно розв'язати наступні задачі: проаналізувати галузі застосування нечітких еталонів (НЕ) в ІБ і визначити вимоги до ФН, обумовлені їх специфікою, на основі чого визначити принципи вибору методу формування ФН для прикладних задач ІБ. Спектр задач обробки НЕ, що розв'язуються в ІБ, визначається галузями застосування автоматизованих систем, що передбачають формування, обробку і отримання висновків щодо об'єктів і процесів систем захисту інформації за допомогою нечітких знань, зокрема, НЕ. Найчастіше НЕ використовуються в системах оцінювання ефективності засобів захисту інформації; в криптографічних системах; в системах «комп'ютерного зору»; в автоматизованих системах

аналізу програмного забезпечення; в системах моніторингу та управління ІБ; в системах управління окремими технічними засобами захисту інформації. Критеріями якості НЕ в у цих системах можна визнати параметри, що впливають на швидкість отримання нечітких характеристик об'єкта і швидкість виконання процедур порівняння, їх здатність забезпечувати визначеність висновку процедур порівняння і можливість використання одного НЕ, сформованого експертним шляхом, в різних системах з різними методами обробки. Крім того, слід враховувати швидкість створення самого НЕ, що визначається кількістю даних, які повинні бути отримані експертним шляхом, швидкістю опитування експертів та кількістю елементарних процедур, які мають бути виконані при формуванні НЕ за певним методом, а також прозорість процедур методу та його вимоги до обчислювальних ресурсів.

Висновки. В даній роботі на основі аналізу особливостей вимог до ФН, обумовлених специфікою застосування НЕ в різних галузях інформаційної безпеки, визначені принципи вибору методу формування функцій належності для прикладних задач інформаційної безпеки і розроблена відповідна методика.

Список літератури:

1. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. — К.: «МК-Пресс», 2006. — 320 с.
2. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1. — Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007. –140 с.
3. Ротштейн А.П. Интеллектуальные технологии идентификации. — Винница: «Универсум Винница», 1999. — 320 с.
4. Турти М.В. Використання однозначної нечіткої логіки в системах технічного захисту інформації //Вісник Східноукраїнського національного університету ім.В.Даля. — 2009. — №6(136). — Ч.1.— С.104–109.
5. Турти М.В. Процедура формування нечітких еталонів на основі попарних порівнянь //Вісник Східноукраїнського національного університету ім.В.Даля. — Луганськ: Вид-во СНУ ім.В.Даля, 2013. — №15(204).— Ч.1. — С.204-209.

Студентка Шемшур А.О., доц. каф. КСЗІ Мелешко О.О.

Національний авіаційний університет, kszi@ukr.net

МЕТОДИ ІДЕНТИФІКАЦІЇ ТА ВСТАНОВЛЕННЯ АВТЕНТИЧНОСТІ

На сьогоднішній день існує досить велика кількість методів ідентифікації та підтвердження автентичності об'єкта. Всі вони різняться способами представлення унікальної інформації та методами її отримання (зчитування). Звичайно універсальної системи захисту, яка б повністю відповідала усім поставленим вимогам не існує.

Найбільш поширеними простими і звичними є методи автентифікації, засновані на паролях — секретних ідентифікаторах суб'єктів. Тут при введенні суб'єктом свого пароля підсистема автентифікації порівнює його з паролем, що

зберігаються в базі еталонних даних в зашифрованому вигляді. У разі збігу паролів підсистема автентифікації дозволяє доступ. Але головним недоліком, так само як і у методах автентифікації, заснованих на використанні унікальних предметів, є людських чинник. Інформацію для запам'ятовування можна забути, а унікальні предмети автентифікації (смарт-карти) можна загубити чи пошкодити, що призводить до втрати часу на їх відновлення. Але цей недолік взагалі не стосується методів автентифікації, заснованих на біометричних параметрах людини.

Біометрична система — автоматизована система, що вирішує задачі реєстрації користувачів та їх ідентифікації. Реалізує наступні функції: фіксація біометричних характеристик; вилучення біометричних даних з вибірки; порівняння біометричних даних з одним або більшою кількістю еталонів; прийняття рішень про відповідність даних; формування результату про справжність. Прикладами впровадження даних методів є системи ідентифікації користувача по малюнку райдужної оболонки ока, відбитками долоні, формам вух, інфрачервоної картини капілярних судин, по почерку, по тембру голосу і навіть по ДНК.

Переваги біометричних систем безпеки очевидні: унікальні людські якості хороші тим, що їх важко підробити, важко залишити фальшивий відбиток пальця за допомогою свого власного або зробити райдужну оболонку свого ока схожою на чиюсь іншу. На відміну від паперових ідентифікаторів (паспорт, водійські права, посвідчення особи), від пароля або персонального ідентифікаційного номера, біометричні характеристики не можуть бути забуті або втрачені, в силу своєї унікальності вони використовуються для запобігання крадіжки або шахрайства.

Головна мета біометричної ідентифікації полягає в створенні такої системи реєстрації, яка вкрай рідко відмовляла б у доступі легітимним користувачам і в той же час повністю виключала несанкціонований вхід в комп'ютерні сховища інформації.

Системи біометричної ідентифікації можна комбінувати, досягаючи астрономічної точності. Найдешевшими і простими у використанні, з хорошою статистикою, є системи допуску по відбиткам і голосу. Допуск по геометрії обличчя зручний і дешевий, але має обмежену область застосувань через погані статистичні показники, також це стосується і геометрії руки. Ідентифікація по підпису так само не є надійним захистом, але якщо поєднати її зі скануванням відбитка пальця. Надійність системи безумовно збільшиться, але пропорційно збільшиться і ціна устаткування.

Статистично надійними і стійкими до підробки є системи допуску по райдужній оболонці. Як відомо райдужна оболонка ока залишається незмінною. Неможливо знайти два абсолютно ідентичних малюнка райдужної оболонки ока, а теоретична ймовірність збігу двох райдужних оболонок становить 1 з 1078. Головним недоліком є дороговизна даних технологій та деякі складнощі з їх використанням. Райдужна оболонка ока вважається найбільш точним біометричний параметром, а значення помилок першого і другого роду у даному методі найнижчі з усіх перерахованих.

Методи ідентифікації та підтвердження автентичності досить відмінні, а їх реалізація призвела до створення широкого та різноманітного ринку технічних засобів, що дозволило, підбираючи та комбінуючи устаткування, створити таку систему захисту, яка б відповідала головним вимогам безпеки.

Щебланін Ю.М. — к.т.н., с.н.с., Левковець Г.С.

Державний університет телекомунікацій

ЗАКОНОДАВЧІ ТА ТЕХНІЧНІ АСПЕКТИ ПЕРЕДАЧІ ЗАКРИТОЇ ІНФОРМАЦІЇ ПО ВІДКРИТИМ КАНАЛАМ

Нормативно-правовий захист інформації являється фундаментом побудови всієї інформаційної безпеки підприємства, організації, установи. В Україні базовими Законами, які регламентують діяльність в інформаційній сфері є:

- Закон України «Про інформацію»;
- Закон України «Про державну таємницю»;
- Закон України «Про Державну службу спеціального зв’язку та захисту інформації України»;
- Закон України «Про телекомунікації»;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та ін.

Взагалі, нормативно-правове забезпечення інформаційної сфери потребує суттєвого удосконалення. Одним з напрямків удосконалення системи інформаційного законодавства України може стати розробка та ухвалення Інформаційного кодексу України, що дозволить розв'язати проблему подолання протиріч у законодавчих та нормативно-правових актах, забезпечити єдність та нефрагментованість нормативно-правового поля.

Аналіз нормативно-правового забезпечення інформаційній сфері виявив деяку його неконкретність та розмитість формулювань. Фактично відсутні визначення конкретних механізмів оприлюднення інформації, конкретних документів, що мають публікуватися. Не встановлюються терміни цієї діяльності, майже відсутні норми прямої дії щодо фінансового та кадрового забезпечення.

В наш час, коли інформація набула стратегічного значення значно гостріше постає питання її безпечної обробки, передачі та використання. Особливо це стосується закритої інформації, доступ до якої має бути обмеженим і захищеним.

В свою чергу це вимагає використання захищених каналів зв'язку на основі сучасних принципів передачі інформації в різних фізичних середовищах таких як:

- дротові канали зв'язку;
- акустичні канали зв'язку;
- канали зв'язку з використанням технологій WiFi і WiMAX (радіоканали).

Забезпечити захист передачі закритої інформації по відкритим каналам можливо після оцінки загроз, які виникають в каналах передачі та методів боротьби з ними.

Дротові канали зв'язку.

Конфіденційна інформація дуже часто передається по телефонних комунікаціях, що пов'язано з оперативністю і зручністю використання цього виду зв'язку. Не зважаючи на все ширше використання для передачі мовної інформації та даних засобів стільникового зв'язку, комп'ютерних мереж, Інтернету, апарати дротового зв'язку наразі залишаються незмінними атрибутами офісних приміщень більшості установ. Слід відзначити, що саме вони відносяться до розряду найменш захищених. І справа не лише в можливості несанкціонованого прослуховування телефонних розмов у режимі реального часу, їхнього запису чи ретрансляції, а й у використанні абонентської телефонної лінії для встановлення телефонних закладок, прослухуванні приміщень у режимі покладеної телефонної трубки, а також використання мережі АТС для живлення засобів технічної розвідки чи передачі по них інформації за межі контрольованих приміщень.

Методи запобігання та протидії поширенню конфіденційної інформації каналами телефонного зв'язку можна класифікувати наступним чином:

- обмеження фізичного доступу до каналів телефонного зв'язку;
- усунення чи виведення з ладу встановлених телефонних закладок;
- впровадження криптографічних методів захисту конфіденційної інформації, що передається засобами телефонного зв'язку.

Акустичні канал зв'язку.

Захист мовної інформації є одним із найважливіших у загальному комплексі заходів технічного захисту інформації. Несанкціоноване ознайомлення із мовною інформацією з метою її подальшого використання є можливим шляхом перехоплення її зловмисниками. Для цього зловмисник може використовувати широкий арсенал портативних засобів акустичної мовної розвідки, які дають змогу перехоплювати мовну інформацію акустичним, віброакустичним, електроакустичним каналами.

Основні з таких засобів можна класифікувати на:

- малогабаритні диктофони, магнітофони та пристрої запису на основі цифрової схемотехніки;
- спрямовані мікрофони;
- електронні стетоскопи;
- оптико-електронні (лазерні) акустичні системи та ін.

Для захисту акустичних каналів зв'язку використовуються спеціалізовані технічні пристрої:

- пристрій захисту «Базальт-1» виробництва «Укрспецтехніки» [1, 2], забезпечує захист мовної інформації від витоку двопроводовими лініями гучномовного зв'язку внаслідок акустоелектричного перетворення в кінцевих пристроях;

- пристрій захисту «Кварц-2» виробництва «Укрспецтехніки» [1, 2], забезпечує генерацію шумових сигналів у звуковому діапазоні частот та ін.

Радіоканали зв'язку.

В радіоканалі основними загрозами (можливими впливами) є:

- перехоплення;

- блокування передачі правової та службової інформації.

Перехоплення може здійснюватися з метою ознайомлення в оперативному порядку з адресованими абоненту повідомленнями.

Найбільш ефективним способом підвищення ступеня захисту інформації є комбінування методів протидії несанкціонованому доступу до інформації, передавався по каналах зв'язку, що представляє собою використання декількох різних способів шифрування.

Література:

1. Державний митний комітет України (Держмитслужба) Лист № 41/16-24-2838-ЕП від 02.06.2004, «Щодо переліку технічних засобів захисту інформації» http://www.gov.lica.com.ua/b_text.php?type=3&id=206903&base=1

2. Технічний захист інформації. http://usts.kiev.ua/price.html.

МЕТОДИ, ЗАСОБИ І ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

УДК 004.621

В.В. Баранник, Ю.Н. Рябуха, С.А. Подлесный, А.Э. Бекиров

АНАЛИЗ ДЕЙСТВИЯ КИБЕРАТАК НА ВИДЕОИНФОРМАЦИОННЫЙ РЕСУРС В ИНФОРМАЦИОННО-ТЕЛЕКОММУКАЦИОННЫХ СЕТЯХ

Стремительное развитие информационных технологий дало возможность широкому распространению передачи мультимедийных данных по таким информационно-телекоммукационным сетям, как системы видеомониторинга и системы видеоконференцсвязи. На сегодняшний момент данные системы используются в государственных ведомственных структурах. Из-за важности передаваемой информации видеоинформационный ресурс может подвергаться кибератакам, что приводит к нарушению целостности и доступности информации.

Наиболее распространенными видами кибератак являются атаки типа DDoS-атака и постановка электромагнитных помех для беспроводных устройств. Распределенная атака типа «отказ в обслуживании» (DDoS-атака) осуществляется с помощью большого количества некорректно сформированных запросов к компьютерной системе или сетевому оборудованию. Она производится на транспортном уровне и имеет своей целью отказ в работе системы из-за исчерпания системных ресурсов. В результате переполнения буфера пакеты будут отбрасываться. Постановка электромагнитных помех для беспроводных устройств осуществляется на физическом уровне. Это атака производится с помощью электромагнитного излучения на линии связи между узлами сети, связанная с

наложением на полезный сигнал шумов, которые приводят к искажению суммарного сигнала. В этом случае в результате несоответствия контрольных сумм пакеты будут отбрасываться. Данные кибератаки приводят к задержкам и потерям пакетов, что в случае предоставления видеоинформационных услуг реального времени внешне проявляется как искажение части или всего кадра, пропадание кадра и замирание кадра. Для предупреждения возникновения атаки типа DDoS-атака могут применяться системы обнаружения и предупреждения вторжений, управляемые коммутаторы со списками контроля доступа и резервирование линий связи между отдельными узлами. Применение систем обнаружения и предупреждения вторжений позволяет контролировать сетевую активность как и на периметре сети так и локально, защитить локальную сеть извне и является наиболее универсальным способом защиты из-за широкого функционала. Применение управляемых коммутаторов со списками контроля доступа позволяет локализировать атаку и блокировать атакующие сегменты вплоть до отдельного хоста. Данный метод эффективный при защите от локальной атаки.

Резервирование линий связи между отдельными узлами является самым простым решением. К недостаткам перечисленных методов являются вносимые из-за обработки пакетов задержки, и как результат ограничение скорость передачи сигнала в сети, увеличенная стоимость оборудования и подписки на сигнатуры, не обеспечивается защита от замаскированных вирусных атак. Для защиты от электромагнитных помех могут применяться широкополосная передача данных, метод скачкообразного изменения несущей и резервирование линий связи между отдельными узлами. Применение широкополосной передачи данных позволяет скрыть факт передачи сигнала, защититься от узкополосной помехи, но метод не работает в условиях применения широкополосного шума. Также ограничивается количество одновременно работающих передатчиков. Метод скачкообразного изменения несущей устраняет недостатки широкополосной передачи, но применение узкополосной помехи приводит к потере пакетов в определенные моменты времени. Резервирование линий связи между отдельными узлами при беспроводной передачи информации не всегда возможно реализовать в связи с тем, что беспроводная связь применяется в случаях невозможности построения «более защищенной» проводной связи.

Вывод: на данный момент не существует методов, гарантирующих абсолютную защиту от кибератак на видеоинформационный ресурс. В информационно-телекоммукационных сетях существует необходимость разработки новых технологий обработки и защиты видеопотока в условиях действия кибератак.

УДК 004.056.5

Н.В. Безмалый
Spf.trade@gmail.com

РИСКИ ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ УСТРОЙСТВ

О мобильных устройствах говорят много и долго. С одной стороны — это чрезвычайно удобно и потому сегодня от смартфона отказаться просто нереально, с другой — использование подобных устройств несет с собой огромные риски. Всегда ли мы их осознаем?

Итак, риски мобильных устройств:

1. Утеря, кража:

1. Украденные смартфоны несут с собой угрозу утраты книги контактов, важных для вас сообщений, да и просто важной информации.

2. Вместе с тем украденное устройство — кладезь информации о вас:

1. Маршруты движения (по времени и датам)

2. Возможность легко установить ваш домашний и рабочий адреса

3. Получить информацию о ваших ближайших друзьях и родственниках

4. Возможно получить вашу персональную информацию вплоть до PIN-кода и номера кредитной карты

5. История ваших страниц в Интернет

6. И многое-многое другое

2. Вредоносное ПО:

1. Рассылка платных SMS

2. Звонки на платные номера

3. Рассылка спама

4. Возможность прослушки (а то и подглядки) за вами

5. Превращение вашего телефона в подслушивающее устройство

6. Рассылка вредоносного ПО

7. Организация DDos атак

8. Да и мало ли что придет в голову злоумышленнику?

3. Утечка информации изнутри компании как по голосовому каналу так и с помощью SMS, MMS, Интернет

4. Утечка корпоративной информации (особенно если используется BYOD).

5. Организация прослушки вашего смартфона

6. Перехват SMS

7. Перехват интернет-трафика, особенно если вы используете Wi-Fi Free

8. Перехват голосового трафика

Что мы имеем на сегодня?

Более трети российских пользователей не задумываются об угрозах для мобильных устройств — таковы данные исследования, проведенного «Лабораторией Касперского» совместно с компанией B2B International.

Неосторожное поведение пользователей может быть объяснено тем, что 38% из них не знают о существовании мобильных киберугроз, а еще 20% знают, но не переживают по этому поводу.

Пользователи нередко хранят ценную информацию на незащищенных мобильных устройствах. Как показали результаты исследования, каждый десятый смартфон на базе Android из числа тех, что не защищены

специальными программами, содержит PIN-коды банковских карт, пароли к системам онлайн-банкинга и прочую финансовую информацию, а в каждом седьмом смартфоне хранятся пароли к социальным сетям, личной и рабочей почте, VPN и другим важным ресурсам. В свою очередь, респонденты, не установившие пароль для доступа к своим телефонам, хранят на них личные письма (30%), рабочие письма (15%) и даже не предназначенные для посторонних данные (8%).

В ходе исследования также выяснилось, что с пользователями Android инциденты случаются даже чаще, чем с пользователями Windows, которые в свою очередь лучше осведомлены о существующей опасности и склонны защищать свои устройства в девяти случаях из десяти. Так, с угрозами за год столкнулись 41% и 50% владельцев смартфонов и планшетов на этой платформе. Учетные записи к онлайн-сервисам были взломаны у 34%, а финансовым кибератакам подверглись 32% пользователей смартфонов и 37% владельцев планшетов Android.

Согласно исследования компании Eset 55% пользователей смартфонов забывают о бэкапах, несмотря на то, что количество владельцев, пострадавших от краж составляет не менее 10% (за последние 12 месяцев).

Таким образом, можно сделать вывод, что с дальнейшим ростом аудитории пользователей мобильных устройств риски будут только расти.

Литература

1. «Лаборатория Каспеского»: 26% смартфонов и 18% планшетов не защищены даже паролем http://www.osp.ru/news/2015/0304/13027712/

2. Eset: 55% пользователей смартфонов забывают о бэкапах http://www.osp.ru/news/2015/0303/13027695/

УДК 629.58: 004.056.53

О.В. Блінцов, В.І. Корицький

Національний університет кораблебудування ім. адм. Макарова,
energybox@mail.ru

ЗАХИЩЕНА СИСТЕМА ІНФОРМАЦІЙНОГО ОБМІНУ СУДНА-НОСІЯ ПРИВ'ЯЗНОЇ ПІДВОДНОЇ СИСТЕМИ

При виконанні підводно-технічних робіт із застосуванням прив'язної підводної системи (ППС) на судні-носії (СН) розгортають елементи ППС [1]: пост енергетики і керування (ПЕК), кабельну лебідку (КЛ) з кабель-тросом (КТ), підводний апарат (ПА).

ПЕК може містити декілька робочих місць: для керівника експедиції, пілота та помічника пілота ПА, оператора маніпуляційного пристрою, оператора-гідроакустика, спостерігачів та інших учасників експедиції. При цьому робочі місця можуть розташовуватись в різних приміщеннях СН.

КЛ з КТ розташовуються як правило на палубі. ПА також розташовують на палубі або в мобільному боксі (ангарі) при виході СН в робочу точку або при проведенні профілактичних робіт.

Виконання підводно-технічної роботи потребує злагодженої взаємодії учасників експедиції: команди СН, екіпажу ППС та інших учасників експедиції (спеціалістів у відповідних галузях), яка неможлива без оперативного голосового та відео зв'язку між ними. Крім того є необхідність в отриманні доступу екіпажу ППС до в першу чергу навігаційної та, можливо, до інших суднових систем, а також до глобальної інформаційної мереж Інтернет. При цьому очевидною є необхідність в забезпеченні захисту інформації, оскільки підводно-технічні роботи можуть виконуватись за комерційним або державним замовленням.

Забезпечити організацію інформаційного обміну на СН з ППС з виконанням означених умов можливо шляхом використання модульної архітектури [2], яка успішно застосовується в багатоцільовій ППС проекту «Гідрограф». Для цього інформаційну систему СН пропонується будувати на основі структури, зображеної на рис. 1.

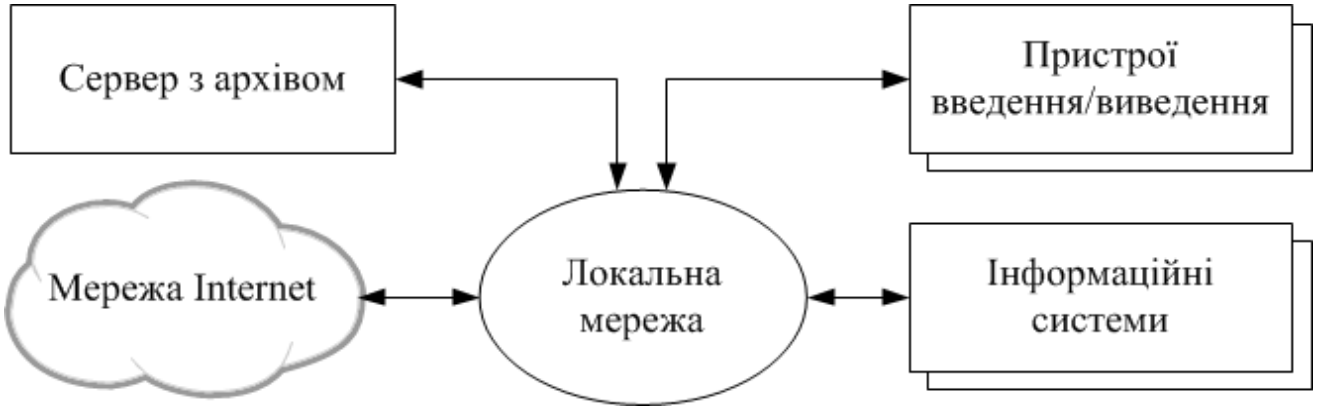


Рисунок 1 — Структура системи інформаційного обміну судна-носія прив'язної підводної системи

До пристроїв введення/виведення відносяться пристрої голосового зв'язку, палубні відеокамери, монітори операторів або спостерігачів. Інформаційні системи — це власне ППС, навігаційна система СН, а також інші системи СН, під'єднання яких до системи інформаційного обміну (СІО) СН виявиться необхідним.

Відеоспостереження на борту СН пропонується будувати на базі цифрових мережевих відеокамер, що зменшить кількість необхідної апаратури та покращить інтеграцію системи відеоспостереження до СІО. Систему голосового зв'язку реалізовано на базі технології VoIP з використанням дротових та бездротових пристроїв голосового зв'язку. Бездротові пристрої голосового зв'язку інтегруються до СІО засобами мережі Wi-Fi. Системи голосового зв'язку та відеоспостереження пропонується виділяти в окремі сегменти мережі СІО, що зв'язані з сервером за допомогою виділених каналів та ізольовані від інших сегментів системи.

Інформаційний обмін між всіма елементами СІО забезпечується сервером із захищеним архівом. На даний елемент системи покладено завдання ретрансляції відео, яке отримано від ПА, забезпечення обміну голосовими

даними між членами екіпажу, організації доступу віддалених клієнтів, які знаходяться в мережі Інтернет до внутрішніх інформаційних ресурсів системи. Центральний сервер системи з'єднано з мережею Інтернет через маршрутизатор з функціями міжмережевого екрану. Такий підхід забезпечить захист сервера та локального сегменту СІО від мережевих атак, що націлені на зменшення доступності інформаційних ресурсів ППС локальним та віддаленим клієнтам.

Більшу частина трафіку, що циркулює в СІО складають пакети з відео- та голосовими даними, які є чутливими до затримок в передачі. Тому обмін даними між вузлами системи пропонується організувати із застосуванням протоколу DTLS. В якості алгоритму шифрування даних обрано блочний алгоритм AES. Такий вибір обумовлений апаратною підтримкою даного алгоритму шифрування багатьма сучасними процесорами, що значно зменшує навантаження на сервер СІО. Інформаційний обмін з віддаленими клієнтами пропонується реалізувати з використанням технології віртуальних приватних мереж. При цьому механізми отримання доступу до інформаційних ресурсів СІО для клієнтів віддаленого та локального сегмента є ідентичними.

Для кожного учасника процесу інформаційного обміну адміністратором системи створюється профіль, який містить перелік прав доступу користувача до певних інформаційних ресурсів системи (потоків від відеокамер, голосових даних, модулів ППС та ін.). Всі спроби отримання доступу до ресурсів протоколюються до захищеного журналу подій, який зберігається на сервері СН. Процес інформаційного обміну між всіма елементами системи має контролюватись з метою недопущення повторного використання інформації, витік якої загрожує інформаційній безпеці системи (відео- та голосові дані, об'єкти, які забезпечують розмежування прав користувачів та ін.). Також сервером виконується періодична діагностика працездатності апаратного та програмного забезпечення, яке входить до складу ППС з протоколюванням процесу до захищеного журналу та оповіщенням адміністратора безпеки у разі виявлення порушень правил безпеки або несправностей в апаратному та/або програмному забезпеченні СІО.

Відеозаписи, а також записи переговорів членів екіпажу ППС, отримані в ході експедиції, зберігаються в захищених архівах, які розміщуються на сервері СІО. Захищені архіви є програмними модулями, які окрім шифрування потоків інформації, отриманої в ході експедиції, виконують моніторинг файлової системи сервера з метою уникнення спроб несанкціонованої її модифікації зловмисником. Записи відео та голосових переговорів екіпажу ППС, при наявності у користувача СІО відповідних прав, можуть бути відтворені локально або експортовані до будь-якого зовнішнього носія, в тому числі до віддаленого вузла в мережі Інтернет.

Висновки

Розроблено структуру захищеної системи інформаційного обміну судна-носія прив'язної підводної системи на основі сучасних мережевих технологій, яка реалізує механізми забезпечення конфіденційності та цілісності інформації, що циркулює як в локальному її сегменті, так і за його межами. В системі передбачено можливості протоколювання подій безпеки та самодіагностики,

що дає змогу більш ефективно виявляти та аналізувати можливі вразливості та спроби несанкціонованого доступу до інформаційних ресурсів системи інформаційного обміну судна-носія прив'язної підводної системи.

Список використаної літератури

1. Блинцов, В.С. Проектирование самоходных привязных подводных систем [Текст] / В.С. Блинцов, В.Э. Магула — К.: Наукова думка, 1997. — 140 с.

2. Блінцов О.В. Концепція створення багатоцільових прив'язних підводних систем з централізованим інформаційним обміном [Текст] / Блінцов О.В. // Восточно-европейский журнал передовых технологий. — Харьков, 2013. — Вып. 6/9 (66). — С. 31-35.

УДК 004.621:681.324

М.М. Браіловський,

Державний університет телекомунікацій, bk1972@ukr.net

ШЛЯХИ ПІДВИЩЕННЯ ЗАХИЩЕННОСТІ МЕРЕЖ ЗА РАХУНОК ЗБІЛЬШЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ

Необхідність створення захищених систем передачі інформації ніколи не викликало жодних сумнівів. Але, на сьогоднішній день, ця проблема в Україні, напевно, набула найбільшого значення за весь час існування країни. Проблемність ситуації ускладнюється ще й тим, що крім «стандартних» проблем створення систем, таких як: надійність, безпека, завадостійкість та ін. [1], ще з'являються економічні та «оперативні» — знання ворогом як принципу дії так і територіального розміщення апаратури захисту. Крім того, необхідно пам'ятати і про людський фактор.

Тому з'являється першочергова задача створення нових структур захищених телекомунікаційних систем, а також алгоритмів та методі прийому, передачі, обробки та збереження даних в них.

Але, зрозуміло, що на розробку і впровадження нового обладнання знадобляться зайві кошти і, головне, — час, що неприпустимо у даній ситуації. Виходячи з цього, стає зрозумілим необхідність розробки нових принципів і алгоритмів роботи існуючого обладнання, які дозволили б за рахунок їх модернізації та не ускладнення апаратури підвищити здатність системи певний час виконувати основні функції, в межах нормативних вимог, при протидії зовнішнім та внутрішнім факторам. Іншими словами, — функціональну життєстійку систему захисту телекомунікаційних систем [2].

Для вирішення проблеми пропонується використовувати новий алгоритм маршрутизації даних у мережах зв'язку. Це дозволить на базі існуючого обладнання (не потрібно нових капіталовкладень) тим самим персоналом (не потрібно перевчати) підняти конфіденційність даних (супротивнику потрібен час на розкриття алгоритму). Відомо, що більша частина часу і ресурсів системи при маршрутизації витрачається на аналіз та вибір оптимального маршруту. Якщо цей маршрут розробити завчасно, то заощадженні ресурси можливо переорієнтувати в інше місце, що в свою чергу вплине на показники функціональної стійкості. Також необхідно підкреслити, що зміна алгоритму

проводиться за рахунок перепрограмування маршрутизатора, що не впливає на роботу обслуговуючого персоналу, а тим самим і не підвищує вірогідність помилок останнього.

Підсумовуючи можливо зробити де які висновки:

- використання нового алгоритму маршрутизації даних дозволить підняти їх захищеність мережах, за рахунок додаткової необхідності відкриття цього алгоритму;
- зміни у операційній системі неодмінно приведуть до зменшення ризику наявності програмних закладок в імпортному обладнанні, що також призводить до підвищення захищеності всієї мережі;
- зміна тільки програмного забезпечення, дозволять не змінювати апаратної частини, а це заощадження коштів і відсутність додаткового некваліфікованого впливу обслуговуючого персоналу;
- ці та інші фактори приведуть до підвищення крім захищеності та ефективності систем і, як наслідок, до покращення функціональних можливостей та життєстійкості мереж зв'язку.

Література:

1. Скоробагатько Е.А., Тимченко Е.В., Хорошко В.А. «Выбор оптимального трафика передачи данных в инфокоммуникационных сетях» \ «Захист інформації» спеціальний випуск: Київ, 2014. — с. 50-59.
2. Браіловський М.М., Хорошко В.О. «Жизнестойкость систем защиты информационного пространства» Телекомунікаційні та інформаційні технології №4, Київ: ДУТ, 2014.—с.41-49.

УДК 004.056

О.І. Бурба

Державний інститут науково-технічної та інноваційної експертизи

СТАН ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОЕКТІВ НАЦІОНАЛЬНОЇ ПРОГРАМИ ІНФОРМАТИЗАЦІЇ ЗА РЕЗУЛЬТАТАМИ ЇХ НАУКОВО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Основним завданням науково-технічної експертизи Національної програми інформатизації та окремих її завдань (проектів) є об'єктивне комплексне дослідження з метою оцінки їх відповідності пріоритетним напрямам державної політики у сфері інформатизації, сучасному рівню татенденціям розвитку інформатизації у світі. Порядок проведення науково-технічної експертизи проектів Національної програми інформатизації визначений постановою Кабінету Міністрів України від 25 липня 2002 року № 1048.

У доповіді наведений аналіз стану забезпечення інформаційної безпеки завдань (проектів) Національної програми інформатизації за результатами проведення їх науково-технічної експертизи, визначені основні недоліки забезпечення інформаційної безпеки при реалізації проектів інформатизації.

Згідно керівних документів один із напрямів проведення експертизи направлений на дослідження відповідності проекту інформатизації вимогам щодо безпеки інформації, у тому числі стосовно криптографічного та технічного захисту. Тобто, кожен з проектів інформатизації, які направлені на створення інформаційних систем або їх модернізації, запровадження систем електронного документообігу, створення та модернізації інформаційних ресурсів, побудови інформаційної інфраструктури, повинен містити у собі аспекти забезпечення інформаційної безпеки.

Як правило, вимоги до реалізації інформаційної безпеки при створенні інформаційних систем формулюються у частковому технічному завданні. Разом з цим, розробники більшості проектів інформатизації враховують вимоги до інформаційної безпеки скоріше формально у відповідних розділах технічних завдань та проектної документації.

Аналіз виконання Національної програми інформатизації свідчить про тенденцію до зростання кількості проектів, які направлені безпосередньо на забезпечення інформаційної безпеки. Так у 2013 році зі 108 проектів інформатизації тільки 3 були направлені на реалізацію інформаційної безпеки. У 2014 році серед 157 проектів питанням інформаційної безпеки присвячено виконання 13 проектів. Можна визначити такі основні напрями їх виконання: створення комплексних систем захисту інформації центральних органів виконавчої влади; закупівля ліцензійного антивірусного програмного забезпечення та систем моніторингу мережевого обладнання відомчих та локальних мереж; закупівля послуг конфіденційного зв’язку та захищеного доступу до мережі Інтернет; закупівля сертифікатів відкритого ключа електронно-цифрового підпису.

Виконання таких проектів повинно відповідати вимогам основних нормативних документів, які регламентують забезпечення інформаційної безпеки: Постанова Кабінету Міністрів України від 29.03.2006 №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»; НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі; НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

В більшості проектів створення комплексних систем захисту інформації разом зі системою розробляються такі документи, як Пояснювальна записка до технічного проекту комплексної системи захисту інформації; Положення про службу захисту інформації; Перелік інформації, що підлягає автоматизованому обробленню та потребує захисту; Опис моделі порушника безпеки інформації; Опис моделі загроз для інформації; Опис політики безпеки інформації; План захисту інформації

УДК 004.942

О.І. Бурба, О.О. Пасічник

Військова частина А1906, oleg_burba@ukr.net

СИГНАТУРНИЙ ПІДХІД ДО МОНІТОРИНГУ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ МОДЕЛІ OSI

Один із основних факторів ефективного функціонування інформаційних систем полягає у забезпеченні комплексної інформаційної безпеки вирішення функціональних і технологічних завдань обробки інформації. Серед сучасних підходів до реалізації інформаційної безпеки виділяють моніторинг відповідних загроз. При цьому під моніторингом розуміють комплексну, цілісну систему заходів, яка призначена для пошуку інформаційних ознак загроз інформаційної безпеки, властивості яких підлягають дослідженню та відображають істотні сторони їх змісту.

В доповіді розглядається сигнатурний підхід до моніторингу загроз інформаційній безпеці інформаційних систем. Сутність такого підходу полягає у понятті співпадіння моніторингової інформації з еталонними ознаками (сигнатурами) загроз інформаційній безпеці функціонування інформаційної системи.

З метою забезпечення комплексності сигнатурного моніторингу загроз інформаційній безпеці аторами пропонується розглядати інформаційні системи з урахуванням принципу їх відкритості. В широкому розумінні відкритою може бути названа будь-яка система (комп’ютер, обчислювальна мережа, операційна система, програмний пакет, інші апаратні чи програмні продукти), яка побудована відповідно до відкритих специфікацій. Під відкритими специфікаціями розуміють опубліковані, загальнодоступні специфікації, що відповідають стандартам і є прийнятими в результаті досягнення згоди після всебічного обговорення всіма зацікавленими сторонами.

Використання принципу відкритості дає змогу обґрунтовано використовувати для класифікації і опису моніторингових сигнатур базову еталонну модель взаємодії відкритих систем (Open Systems Interconnection basic reference model — OSI). В моделі OSI під відкритою системою розуміють мережевий пристрій (вузол), що може взаємодіяти з іншими мережевими пристроями (вузлами) з використанням стандартних правил — протоколів, які визначають формат, зміст і значення прийнятих чи відправлених повідомлень. Тому, інформаційні системи в нотації OSI можна надати сукупністю протоколів, які використовуються на відповідних рівнях взаємодії.

Враховуючи зазначене, сигнатурний моніторинг полягає у визначенні сукупності ознак загроз інформаційній безпеці на рівнях протоколів моделі OSI і побудові на їх основі відповідних сигнатур. В якості ознак загалом можна розглядати специфікацію протоколів, які на кожному рівні деталізуються відповідними значеннями пакетів, кадрів, байтів.

З урахуванням цього для виявлення сигнатур можуть використовуватися такі підходи.

1) Збіг з шаблоном. Виявлення базується на пошуку фіксованої послідовності байтів в розглянутому елементі даних мережевого трафіку (наприклад, одиничному пакеті). Ці сигнатури містять деякі ключові слова або вирази.

2) Збіг з шаблоном стану. По одному пакету встановлюється стан потоку даних. Поява іншого пакета (або пакетів), який не відповідає даному стану, вважається аномалією.

3) Аналіз на основі шаблону протоколу. Для формування сигнатури використовується декодування різних елементів протоколу. При декодуванні протоколу здійснюється порівняння з правилами, які визначені як порушення.

4) Контроль частоти подій або перевищення граничної величини. Ці сигнатури описують ситуації, коли протягом деякого інтервалу часу відбуваються події, кількість яких перевищує задані заздалегідь показники.

Таким чином у доповіді розглянуто сигнатурний підхід до виявлення ознак загроз інформаційній безпеці функціонуванню інформаційних систем, який забезпечує комплексність моніторингу за рахунок використання моделі OSI.

УДК 621.391.7

В.М.Бурлаков, В.М.Домрачев, В.В.Третиник

НТУУ «КПІ», «Європейський університет», м. Київ, mipt@ukr.net

ВИДОБУВАННЯ ІНФОРМАЦІЇ З ДАНИХ (DATA MINING), КІБЕРБЕЗПЕКА ТА ЗАПОБІГАННЯ ШАХРАЙСТВУ

Обробка даних є одним з найважливіших напрямків розвитку інформаційних технологій. Методи інтелектуальної обробки даних знайшли впровадження у обробці здебільшого слабо структурованих даних, які, зокрема, мають великий обсяг. Це такі напрямки досліджень, як радіофізика, астрофізика, обробка та розпізнавання сигналів, біомедицина, фінанси та кібербезпека [1, 2].

Поточний стан економіки України, вплив агресії з боку Росії та останні події на світовому фінансовому ринку потребують особливої уваги з боку інформаційної безпеки. До вирішення цієї задачі підключились такі відомі комп'ютерні компанії як IBM (Cognos Express, SPSS), Microsoft, SAS та інші.

Зокрема компанія SAS активно пропонує на ринку інструменти SAS Enterprise Miner, які дозволяють вирішувати багато задач пов'язаних з запобіганням кіберзлочинності.

Серед основних задач — задачі обробки текстової інформації: контроль за змістом блогів та web-сайтів, який дозволяє своєчасно реагувати на колективні настрої населення.

Системи Data mining дозволяють аналізувати частотні характеристики правопорушень та враховувати ці аналізи при прогнозуванні та при розробці процедур їхнього запобігання.

Моніторинг сплати клієнтами податків та виявлення шахрайства у цьому напрямку є важливим для наповнення державного бюджету.

SAS Enterprise Miner включає інструменти боротьби з несанкціонованим вторгненням в комп'ютерну мережу, виявлення цих вторгнень та їх своєчасного блокування.

Завдяки наявності у кіберінфраструктурі великої кількості даних стійко зростає кількість злочинців, що намагаються отримати доступ до даних. Системи Data mining використовують результати машинного навчання, статистичного аналізу, штучного інтелекту, і розпізнавання образів даних для того, щоб класифікувати та ідентифікувати поведінку шахраїв, для нетривіального прогнозу несанкціонованого вторгнення в комп'ютерну мережу.

Інструменти Data mining мають важливе значення при боротьбі з комп'ютерними хробаками. Принципи покладені у боротьбі з комп'ютерними хробаками полягають у побудові методів попередньої їх класифікації та виявлені характерних програмних кодів. Після визначення цих програмних кодів методи боротьби з комп'ютерними хробаками проходять тестування на контрольованих учбових даних з метою визначення можливості запобігання застосування прихованих функцій пошкодження процесу обробки даних.

Аналізуючи код програми методи боротьби з комп'ютерними хробаками надають можливість використовуючи евристичні алгоритми аналізу своєчасно виявляти цих хробаків (вірусів) та вносити у код програми зміни, які нейтралізують їх шкідливий вплив.

Особливе значення системи Data mining мають для фінансових корпорацій, зокрема банків. Це своєчасне запобігання спробам шахрайства при наданні банками кредитів (кредитний скоринг) та аналіз (моніторинг) переказу коштів з використанням платіжних карток.

Список використаних джерел:

1. Sumeet Dua. Data Mining and Machine Learning in Cybersecurity / Sumeet Dua, Xian Du. — Taylor & Francis Group, 2011. — 223 p.

2. Домрачев В.М. Система підтримки прийняття рішення з інформаційної безпеки організації / В.М. Домрачев // Збірник тез доповідей VII Міжнародної науково-технічної конференції «Сучасні інформаційно — комунікаційні технології» — К.: ДУІКТ. –2011. — С. 126.

УДК 004.056.5

Г.В. Гаврилюк

Київський національний університет імені Тараса Шевченка, Graf1997@mail.ua

ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

В останні роки багато компаній добре усвідомили необхідність управління інформаційною безпекою підприємства. Ефективне управління питаннями інформаційної безпеки набуває все більшого значення для компаній по мірі їх зростання і просування на нові ринки товарів і послуг. Клієнтам важливо знати, що дотримується конфіденційність їхніх персональних і ділових даних. Інвесторам необхідна впевненість в тому, що бізнес та інформаційні активи компанії захищені. Ділові партнери очікують, що компанія буде

функціонувати без збоїв, які можуть бути викликані помилками в роботі інформаційних систем, навмисними або ненавмисними діями персоналу, шкідливим програмним забезпеченням та іншими факторами.

Управління інформаційною безпекою — це комплекс заходів, які ґрунтуються на підході, що враховує бізнес-ризики, призначені для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Побудова ефективної системи управління інформаційною безпекою — це не разовий проект, а комплексний процес, наплавлений на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси і час.

Для побудови ефективної системи інформаційної безпеки необхідно спочатку описати процеси діяльності. Потім слід визначити поріг ризику — рівень загрози, при якому вона потрапляє в процес управління ризиками. Потрібно побудувати таку систему інформаційної безпеки, яка забезпечить досягнення заданого рівня ризику.

Організаційно-правові види порушень — це порушення, пов'язані відсутністю єдиної узгодженої політики компанії в сфері захисту інформації, невиконанням вимог нормативних документів, порушенням режиму доступу, зберіганням і знищення інформації.

Інформаційні види порушень включають несанкціоноване отримання повноважень доступу до баз і масив даних, несанкціонований доступ до активного мережного обладнання, серверів доступу, некоректне застосування засобів захисту і помилки в управлінні ними, порушення в адресності розсилки інформації при веденні інформаційного обміну.

Фізичні види порушень включають фізичне пошкодження апаратних засобів автоматизованих систем, ліній зв'язку і комунікаційного устаткування, крадіжки або несанкціоноване ознайомлення з вмістом носіїв інформації, що зберігаються в неналежних місцях, розкрадання носіїв інформації, відмови апаратних засобів та ін.

До радіоелектронних видів порушень відносяться такі порушення, як впровадження електронних пристроїв перехоплення інформації, отримання інформації шляхом перехоплення і дешифрування інформаційних потоків, дистанційна відеозапис (фотографування) моніторів, комп'ютерних роздруківок, клавіатури, нав'язування неправдивої інформації в локальних обчислювальних мережах, мережах передачі даних і лініях зв'язку.

Криптографія підвищує рівень інформаційної безпеки підприємства і знижує ризик витоку приватної інформації.

Стеганогра́фія — тайнопис, при якому повідомлення, закодоване таким чином, що не виглядає як повідомлення. Таким чином непосвячена людина принципово не може розшифрувати повідомлення, бо не знає про факт його існування.

УДК 004.056.5

Ю.А. Гірік
НТУУ «КПІ», Факультет електроніки, Київ, Україна,
e-mail: giyuriu@gmail.com

ВТРАТИ ВІД ВИТОКУ ІНФОРМАЦІЇ

XXI століття, мабуть, взагалі називатимуть ерою інформації і комунікації. Вони починають відігравати дедалі все більшу роль, і внаслідок цього все масштабніше стає використання технічних засобів для охорони інформації, комп'ютерної техніки, мережі Інтернету, та хмарних обчислень, які сконцентрували надзвичайну кількість інформації часто конфіденційної або навіть секретної. Сучасні носії інформації стають дедалі більш компактними, і в них не тільки акумулюються значні об'єми інформації, вони до того ж дозволяють майже непомітно її передавати.

Сьогодні втрати інформації носять, як фінансові, так і репутаційні складові, а крадіжки інформації привертають величезну увагу з боку підприємців і суспільства в цілому. Перших лякають можливі втрати, які здатні привести до банкрутства, других — цікавить професійний аспект, треті занепокоєні можливостями згадування їх в пресі. Витоки особистої інформації клієнтів різноманітних компаній зростають і це спричиняє фінансові і моральні втрати для них, обсяги цих втрат зростають кожен рік.

Найбільш складними для розрахунків є витоки інформації як інтелектуальної власності, військових технологій та тих, що шкодять безпеці та репутації країни. Все це негативно впливає на інвестиції, репутацію країн і їх компаній на міжнародній арені.

Ґрунтуючись на даних проведеного аналізу та використаних джерел, можна зробити висновок що застосування систем технічного захисту інформації дозволяє знаходити та ліквідовувати до 90% усіх спроб їх несанкціонованого отримання, особливо утаємниченої інформації, та зменшення витрат від витоків у грошовому еквіваленті від 5 до 200 млн. доларів США на рік в залежності від розміру та обороту компанії.

Використані джерела:

1. Net Losses:Estimating the GlobalCost of Cybercrime. Economic impact of cybercrime II.McAfee

2. 2013 Cost of Data Breach Study:Global Analysis. Ponemon Institute.

3. Verizon's 2014 Data Breach Investigations Report.

4. Конституція України. Закон України про захист інформації. Розділ V. Стаття 17.

5. Cyber Security Spending in Critical Infrastructure to Hit $46 Billion Globallyv. ABI Research

УДК 621.376.54

О.О. Головко, В.П. Новіков, проф.

Державний університет телекомунікацій

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЗАСТОСУВАННЯ FUZZY-ТЕХНОЛОГІЙ

Реальною альтернативою та доповненням до базових методів оцінки рівня захисту інформації комплексних систем захисту інформації (КСЗІ) є застосування у дослідженнях Fuzzy-технологій, які дозволяють проводити оцінку за умов слабкої визначеності оціночних факторів та їх різнорідності. Вони уможливлюють аналіз значної кількості якісної інформації, отриманої від експертів та доповненої кількісними даними. Fuzzy-технології є сукупністю теоретичних основ, методів, алгоритмів, процедур і програмних засобів, що базуються на використанні теорії нечітких мір (ТНМ) і оцінок експертів для вирішення широкого класу задач з самих різних областей [1,2]. Теорія нечітких мір, нечіткої логіки або *Fuzzy Logic* — новий підхід до опису процесів, в яких присутня невизначеність, що ускладнює і навіть виключає вживання точних кількісних методів і підходів. Основна відзнака методу — введення лінгвістичних змінних (суб'єктивних категорій) і методів їх обробки. Ця теорія може виступати як інструмент моделювання невизначеності, який базується на відомій розумовій здатності людини оперувати якісними категоріями і оформляти свої логічні висновки також в якісній формі.

Застосування даної технології підвищує достовірність і якість рішень, що приймаються, при суттєвому зниженні вимоги до вхідних даних (їх якості, кількості, достовірності), формалізація яких виконується настільки точно, наскільки дозволяє їх обсяг і якість.

Крім того, існує ще декілька причин використання ТНМ. По-перше, нечіткі множини ідеально описують суб'єктну активність посадової особи, що приймає рішення щодо введення КСЗІ в експлуатацію. По-друге, нечіткі числа ідеально підходять для планування факторів у часі, коли їх майбутня оцінка ускладнена (розмита, не має достатніх імовірнісних умов). Таким чином, всі сценарії за тими чи іншими окремими факторами можуть бути зведені в один сценарій у формі трикутного числа, де відокремлюють три позиції: мінімально можливе, найбільш очікуване та максимально можливе значення фактору. Причому ваги окремих сценаріїв у структурі зведеного сценарію формалізуються як трикутна функція приналежності рівня фактора нечіткій множині «приблизного рівняння середньому». По-третє, при використанні нечітких множин ми можемо в межах однієї моделі формалізувати особливості застосування ОІД [4].

Математичні моделі на основі Fuzzy-технологій набули широкого розповсюдження для вирішення задач в електроніці, кібернетиці, управлінні складними інтелектуальними системами. Більшість з таких завдань відносяться до класу експертно-аналітичних завдань (ЕАЗ) оцінки і прогнозу стану КСЗІ, вирішення яких повинне базуватися на методах системного аналізу, експертній методології і перспективних математичних методах обробки даних.

Таким чином, Fuzzy-технології дозволяють проводити оцінку за умов слабкої визначеності оціночних факторів та їх різнорідності, створювати математичні моделі оцінки КСЗІ за цільовою спрямованістю; багаторівневою за ієрархічною структурою; аналітичною за способом опису функціональних зв'язків; імовірнісною з точки зору врахування стохастичної невизначеності; комбінованою за способом урахування випадкових факторів (реалізовані детермінований та стохастичний підходи з урахуванням нестохастичної невизначеності); за характером вихідної інформації такою, що використовує методи обробки нечітких даних.

УДК 004.056.5

С.Ф. Гончар, к.т.н., Г.П. Леоненко, к.т.н., О.Ю. Юдін

Державний НДІ Спецзв'язку, sfgonchar@gmail.com

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Багато держав, в першу чергу економічно розвинуті, вдосконалюють методи та способи використання інформаційних технологій і засобів для деструктивних інформаційних впливів на інформаційні системи об'єктів критичної інфраструктури (ОКІ). Під ОКІ будемо розуміти атомні і гідроелектростанції, нафто — і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, загальнодержавні системи зв'язку, галузеутворюючі підприємства тощо [1]. Тому, безпеку ОКІ необхідно розглядати в новому ракурсі, а саме: разом з класичними заходами безпеки, необхідно забезпечувати їх інформаційну безпеку.

Очевидно, що в умовах сучасного надзвичайно інтенсивного розвитку інфраструктури провідних країн світу існує багато ОКІ, виведення з ладу яких може призвести до надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, заподіянням великих матеріальних та економічних збитків.

Викладене вище показує, що питання забезпечення інформаційної безпеки ОКІ держави являється актуальною задачею.

Визначаючи основні завдання забезпечення інформаційної безпеки ОКІ можна зазначити, що першочерговим є завдання створення дієвого механізму координації зусиль органів влади та підрозділів організацій, які повинні забезпечувати інформаційну безпеку відповідних об'єктів [2].

Крім того, необхідно впроваджувати ряд істотних заходів на державному, регіональному та галузевому рівнях з організаційного, нормативно-правового та науково-методичного забезпечення.

Як показує досвід розвинутих країн, дослідження механізмів захисту інформації ОКІ включає на перших кроках етап ідентифікації (визначення) елементів, які повинні розглядатися в якості об'єктів критичної інфраструктури. Разом з тим важливим напрямком забезпечення захисту інформації на об'єктах

критичної інфраструктури є запровадження відповідного управлінського впливу.

Проведений детальний аналіз показує недостатність національних та галузевих стандартів щодо забезпечення інформаційної безпеки ОКІ України. Крім того, зазначені стандарти повинні бути гармонізовані із міжнародними стандартами.

Враховуючи викладене, можна зазначити, що основними завданнями із забезпечення безпеки інформації на ОКІ держави мають бути:

- нормативно-правове регулювання у сфері забезпечення безпеки інформації на ОКІ держави;
- визначення загроз безпеки інформації і виявлення уразливостей в програмному і апаратному забезпеченні ОКІ держави;
- оцінка реальної захищеності ОКІ держави;
- розробка вимог по забезпеченню безпеки інформації в критичній інфраструктурі держави;
- розробка та реалізація заходів по забезпеченню безпеки інформації на ОКІ держави;
- здійснення контролю і нагляду в галузі забезпечення безпеки інформації на ОКІ держави;
- інформаційне, матеріально-технічне і науково-методичне забезпечення безпеки інформації на ОКІ держави;
- підготовка та перепідготовка фахівців в області забезпечення безпеки інформації на ОКІ держави.

Список використаних джерел:

1. Леоненко Г.П., Юдин А.Ю. Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины // Information Technology and Security. -2013. — Вип. 1(3). — С. 44.

2. Гончар С.Ф. Шляхи удосконалення державної політики забезпечення інформаційної безпеки критичної інфраструктури України : матеріали круглого столу «Державне реагування на загрози національним інтересам України: актуальні проблеми та шляхи їх розв’язання». — К.: НАДУ, 2014. — С. 92-95.

УДК 338.47:65.012.8

В.Д. Данчук, д.ф.-м.н., О.Є. Ананченко, В.Є. Ананченко

Національний транспортний університет,ozzzborn.aa@gmail.com

УДОСКОНАЛЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНХ СИСТЕМ

Планування, впровадження та забезпечення діяльності Security Operations Center (SOC) в його традиційному розумінні — як ситуаційного центру моніторингу та управління інцидентами інформаційної безпеки — є сьогодні одним з актуальних завдань ефективного функціонування корпоративних інформаційних систем (КІС) із складною ІТ-інфраструктурою. Тут, в сучасних умовах високого динамізму отримання, обробки та реалізації інформації

виникає нагальна потреба у централізованому онлайн-моніторингу подій у різноманітних джерел КІС з відображенням у режимі реального часу, кореляції результатів, надання відповідних звітів та попереджень, що дає змогу забезпечити відповідальний персонал та користувачів повною інформацією про її стан і тим самим забезпечити можливість ефективно управляти ризиками системи. Найбільш ефективним підходом для вирішення такого класу задач, на наш погляд, уявляється використання сучасних систем управління інформацією та повідомленнями безпеки (Security Information and Event Management (SIEM)) [1].

В роботі об'єктом дослідження слугувала КІС «Наука в університетах», що розроблена Національним транспортним університетом та впроваджена в МОН України. Ця система призначена для автоматизованого супроводу наукових проектів ВНЗ та наукових установ (НУ) на етапах їх формування, проведення конкурсу, експертизи, звітної компанії. Особливістю клієнт-серверної архітектури КІС є реалізація двох типів (веб- та віконного) додатків, кожен з яких має відповідні типи інтерфейсів: користувацький та адміністративний. У відповідності до типу додатку та інтерфейсу КІС «Наука в університетах» забезпечує прозорість та об’єктивність конкурс проектів; он-лайн режим створення проектів для проходження щорічного конкурсного відбору, експертизи проектів та звітів по проектам, звітування по проектах та науковій та науково-технічній діяльності ВНЗ та НУ в цілому; автоматизований (об’єктивний) розподіл експертів для проведення експертизи; автоматизовану підготовку пакету документів засідання секцій для МОН України; формування рейтингових показників проектів та їх виконавців; автоматизоване формування тематичних планів та фінансової звітності; підготовку звітних та аналітичних матеріалів.

За основу реалізації запропонованого підходу захисту інформації КІС «Наука в університетах» був вибраний продукт AlienVault Open Source SIEM (OSSIM) [3], що являє собою повноцінну безкоштовну відкриту SIEM-систему. AlienVault OSSIM забезпечує усю функціональність, яка вимагається для детектування та профілювання атак, і забезпечує всебічну інтелектуальну платформу управління безпекою з набором відповідних інструментальних засобів.

Список використаних джерел:

1. Mosaic Security Research. Log Management & Security Information and Event Management (SIEM)// https://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management.

2. Данчук В.Д. Синергетична корпоративна інформаційна система управління проектами та програмами/ В.Д. Данчук, Ю.С. Лемешко, Т.А. Лемешко// Управління проектами, системний аналіз і логістика: Науковий журнал. Вип.9. –К. : НТУ, 2012. — С.51 — 53.

3. AlienVault Open Source SIEM (OSSIM) // http://www.alienvault.com/.

УДК 354.42

С.Я. Довбня[1],к.в.н., доцент, **В.М. Бурлаков**[2], к.т.н, доцент., **О.В. Драний**[2]

Київський національний університет [1], ДП НАЕК «Енергоатом [2]

,dovbnja.sergej@i.ua

ПРАКТИЧНІ АСПЕКТИ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІТС

Комплексна система захисту інформації в інформаційно-телекомунікаційній системі (ІТС), відповідно до законодавчих та нормативних вимог України повинна забезпечувати захист від несанкціонованого доступу (НСД) та, у разі використання незахищених каналів зв'язку між компонентами ІТС за межами контрольованих зон, здійснювати криптографічний захист конфіденційної інформації, що передається цими каналами.

Проведення практичних заходів з побудови КСЗІ в складній корпоративній ІТС класу 3, в частині якої обробляються персональні дані, виявило декілька проблемних моментів, пов'язаних з урахуванням таких особливостей структури ІТС, яка:

- містить групи доменів, в яких обробляються персональні дані,різних ієрархічних рівнів — центрального рівня та відокремлених підрозділів організації;
- знаходиться у стані постійного розвитку, та не є статичною. Її розвиток здійснюється не централізовано, а за потребами та відповідними рішеннями центрального рівня та відокремлених підрозділів;
- через особливості виконуваних персоналом функцій повинна враховувати неможливість відключення сегментів, що оперують персональними даними, від глобальних мереж.

На етапі проведення обстеження середовища, в якому здійснюється обіг персональних даних (ПД), місць і форматів зберігання даних, виділені відповідні сервери баз даних, маршрути та робочі станції користувачів в сегментах ІТС за принципом максимальної локалізації, а також визначені наявні технічні та програмні засоби, що можуть бути застосовані для технічного захисту інформації.

З метою мінімізації коштів при реалізації захисту від НСД серверів та робочих станцій ІТС прийнято рішення щодо використання сервісів безпеки операційних систем Windows, підтримка яких буде здійснюватись виробником протягом не менш п'яти перших років експлуатації створюваної КСЗІ (пов'язано з критичними для безпеки оновленнями). Для встановлення відповідності обчислювальної потужності технічних засобів вимогам щодо впровадження вищезазначених операційних систем проведено необхідну модернізацію низки окремих робочих станцій ІТС.

Оновлення серверних частин ІТС вимагало суттєвих витрат, що наштовхнуло на рішення щодо централізації — зміни існуючої структури шляхом зведення її до єдиного домену та загального серверу баз даних як для центрального рівня так і для відокремлених підрозділів організації. Централізація серверної частини призвела до можливості управління ІТС

єдиною службою захисту інформації, скорочення місць зберігання ПД та осіб з адміністративними правами доступу.

Вибір засобів криптографічного захисту інформації (КЗІ) здійснювався за критеріями достатньої пропускної спроможності при мінімальній вартості, що передбачало їх тестування. Архітектуру прийнятого рішення та його характеристики наведено на рис. 1 та в таблиці 1.

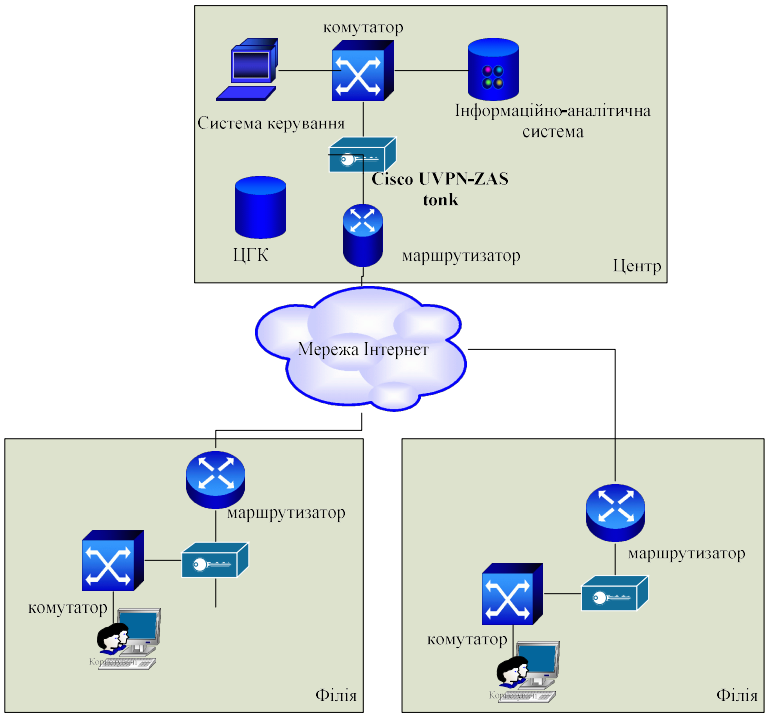


Рис. 1 Архітектура прийнятого рішення

Під час проведення тестування різних засобів КЗІ з'ясувалося, що стійкість алгоритму шифрування, та пропускна спроможність засобу КЗІ не є виключними критеріями для прийняття рішення про можливість їх використання. Так в реальних умовах діючої ІТС, деякі засоби КЗІ порушували протокол обміну даними між клієнтом та сервером баз даних ERP — системи, спричиняючи непрацездатність важливих бізнес-процесів. При цьому досить складно знайти істинну причину несумісності між засобами КЗІ та вендором ERP-системи.

Оскільки захищений сегмент ІТС не є статичним, однією з основних вимог до його структури є забезпечення можливості модернізації без проходження додаткових експертиз КСЗІ.

Таблиця 1.

Можливість	***«Комплекс програмний КЗІ Cisco UVPN-ZAS»*** (Шлюз)
Стабільність роботи	Так
Масштабованість	У випадку, якщо кількість майданчиків буде перевищувати 10 потребує модернізації у центрі, та відповідно, додаткове придбання компонентів рішення безпосередньо на майданчику

Можливість реалізації відмовостійкого рішення	Так (у випадку встановлення додаткового компоненту для центру)
Можливість функціонування через Nat	Так
Пропускна здатність	до 25 Мбіт/сек
Можливість балансування навантаження	Так
Вбудований фаєрвол	Так
Можливість тонкого налаштування трафіку (різні правила блокувань і пропускання /шифрування/ трафіку в залежності від архітектури системи і необхідності захисту)	Так

В обраному варіанті рішення це можливо провести шляхом розроблення порядку розгортання додаткових робочих місць, зміни структури об'єктів захисту, за умови використання у зміненій топології системи засобів технічного захисту та їх налаштувань, однотипних з тими, що пройшли державну експертизу в первинному складі КСЗІ.

УДК 621.391.54

М.П. Дудка

Державна прикордонна служба України, maxim_dudka@ukr.net

к.т.н., доцент І.О. Четверіков

Київський національний університет імені Тараса Шевченка, ivan-chetverikov@yandex.ua

БЕЗПЕКА В СУЧАСНИХ МЕРЕЖАХ IP ТЕЛЕФОНІЇ

Технологія передачі голосу по мережах IP отримала саме широке поширення для спілкування. Тривають розробки пристроїв і програмного забезпечення для цієї перспективної технології. IP телефонія займає перші місця по реалізації в телекомунікаційних системах компаній, корпорацій, державних установ, операторів і провайдерів. Традиційні системи телефонії (аналогові, гібридні, цифрові) перейшли на задній план, витісняються більш інноваційними рішеннями.

Для роботи IP телефонії потрібно:

Транспорт — мережа Ethernet з використанням стека протоколів TCP / IP. Протокол UDP переважніше протоколу TCP.

Для комутації та обслуговування дзвінків використовуються IP PBX (IP ATC). Оператори для обслуговування дзвінків використовують програмний комутатор (Softswitch) 5-го класу.

Крім офісних, комерційних і операторських рішень існують також Internet користувальницькі. До них можна віднести Skype, Viber та ін.

IP-телефонії є свої переваги та недоліки.

Плюси:

• можливість переадресації дзвінків по IP-мережі;

• підключення до мережі можливо з будь-якої точки світу, де є Інтернет;

• ваш телефонний номер зберігається в будь-якій точці світу;

• дзвінок дешевше, ніж через дорогі міжміські телефонні лінії.

Мінуси:

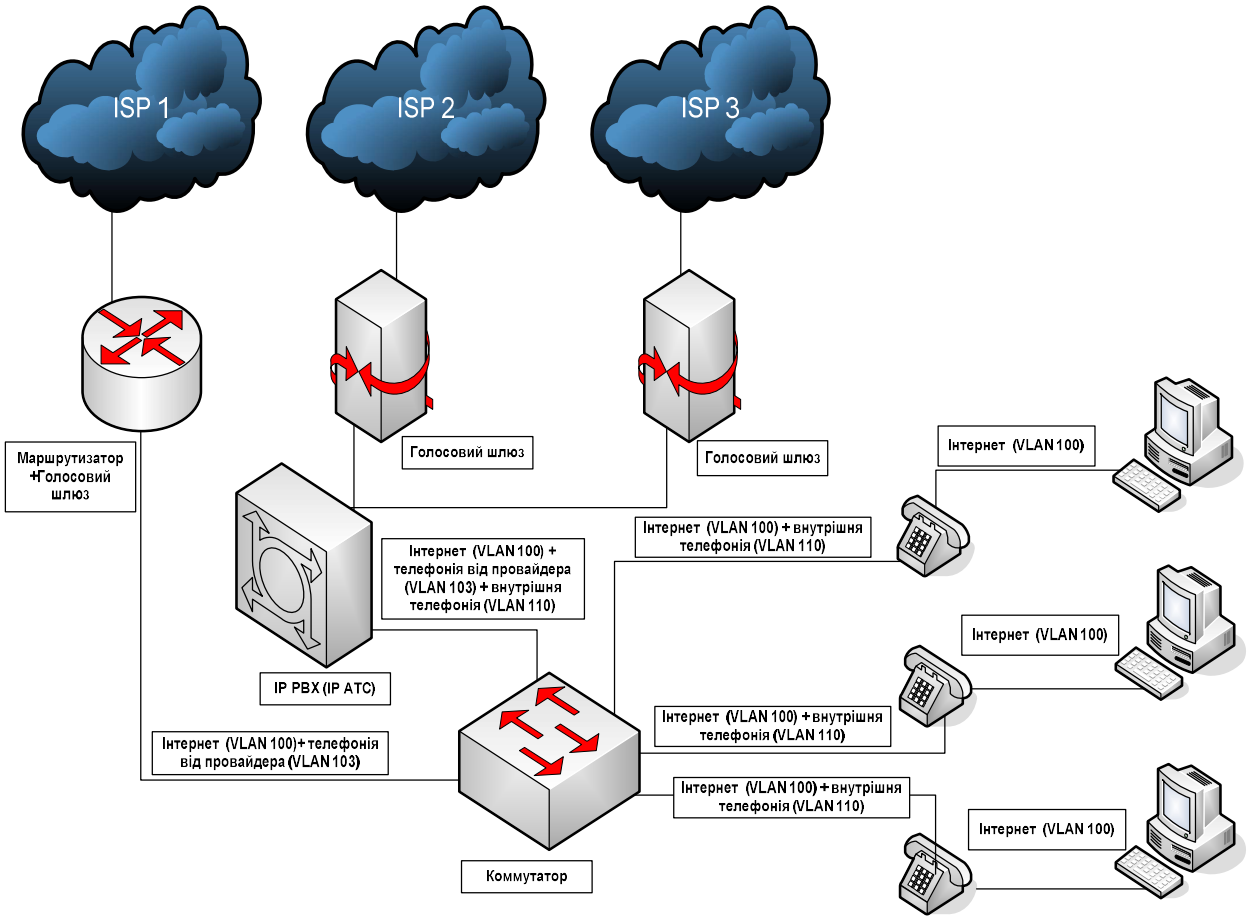
• у оператора може не бути виходу на телефонну мережу кінцевого населенного пункту, куди ви телефонуєте;

• дзвінки в екстрені служби (101, 102, 103, 104) можуть не проходити, так як складно визначити географічне положення об'єкта;

• через IP-мережу можуть проникати віруси, корпоративна мережа може бути атакована порушниками.

Безпека — це вимога і, з іншого боку, характеристика системи зв'язку, телекомунікаційної системи, і безпосередньо голосового трафіку. Основні питання безпеки IP телефонії в телекомунікаційній мережі це злом і генерування телефонного трафіку. Найбільш цікаві для порушників (зловмисників) голосові шлюзи. Вони не володіють механізмом визначення «кому куди можна дзвонити».

Не залишаються без уваги і самі IP PBX (IP ATC). Особливо користуються великим попитом у зловмисників ті, що мають відкритий код. Компанії розробники IP PBX (IP ATC) витрачають чимало коштів, для захисту своїх продуктів від злому, як з боку адміністрування продукту, так і з боку абонентських підключень.



Що стосується безпеки безпосередньо самого голосового трафіку, то це перехоплення пакетів і тим самим підслуховування розмов. Або ж за допомогою програм аудіо обробки, заміна або підміна слів / словосполучень.

Які основні способи забезпечення безпеки IP телефонії в телекомунікаційних мережах? Правилами безпеки і в той же час забезпечення якості обслуговування (QoS) рекомендується в телекомунікаційній мережі використовувати VLAN'и.

Для того, щоб дзвінки контролювалися і прямували згідно аутентифікації, правам доступу та правилам маршрутизації, все обладнання телефонії має реєструватися на пристрої управління. Таким пристроєм є IP PBX (IP ATC). Для реєстрації абонентських пристроїв використовуються як відкриті протоколи: SIP, H.323, так і пропрієтарні SCCP (Skinny Client Control Protocol Cisco Systems Inc.). Для реєстрації голосових шлюзів використовуються протоколи: SIP, H.323, MGCP, H.248 / MEGACO.

Забезпечення безпеки в IP телефонії досягається вирішенням цілого ряду завдань. Виділення голосового трафіку в окремий VLAN для підвищення якості обслуговування та безпеки. Виділення єдиного пристрою управління дзвінками забезпечить контрольованість і розмежування прав для здійснення дзвінків за різними напрямками. Замикання всіх голосових шлюзів на IP PBX (IP ATC) за протоколами MGCP, H.248 / MEGACO — забезпечить захист і неможливість здійснення генерування несанкціонованих дзвінків. Прив'язка всіх пристроїв по MAC адресам і подальша реєстрація. І, нарешті, використання протоколів шифрування.

УДК 004.056.55

М. В. Єсіна

Харківський національний університет імені В.Н. Каразіна, факультет комп'ютерних наук, кафедра безпеки інформаційних систем і технологій, bist@karazin.ua

МЕТОДИ ТА ПРИНЦИПИ АВТЕНТИФІКАЦІЇ В ЕЛЕКТРОННІЙ ІДЕНТИФІКАЦІЇ

Розвиток систем електронної інформаційної взаємодії, інфраструктури електронного документообігу, є актуальним завданням для України, що і знайшло відображення у Програмі економічних реформ на 2010-2014 роки «Заможне суспільство, конкурентоспроможна економіка, ефективна держава», затвердженій Указом Президента України від 12.03.2013 №128/2013. Побудова електронного інформаційного суспільства насамперед спирається на довіру, необхідну для взаємодії всіх об'єктів та суб'єктів інформаційного суспільства. Зважаючи на вищезазначене, актуальності набуває задача розпізнання особистості, відокремлення її серед безлічі інших. Механізм реалізації зазначених задач отримав назву ідентифікації.

Метою цієї роботи є аналіз методів, принципів та понять електронної ідентифікації і автентифікації.

Ідентифікація — процес присвоєння суб'єкту чи об'єкту унікального позначення — імені чи коду, характерної ознаки, наявність якої дозволяє виділити даний об'єкт (суб'єкт) серед множин інших, а також процес пред'явлення суб'єктом чи об'єктом цього ідентифікатора.

Електронна ідентифікація означає процес використання персональних даних ідентифікації в електронній формі, які однозначно визначають фізичну або юридичну особу.

У тексті прес-релізу Регламенту зазначено, що електронна ідентифікація — це процес однозначного визначення ідентичності людини/особи за допомогою використання електронних засобів.

В останній редакції проекту Закону України «Про електронний цифровий підпис» надане наступне визначення поняття автентифікації. Автентифікація — це електронний процес, який дозволяє підтвердити належність ідентифікаційних даних фізичній або юридичній особі, інформаційній системі, походження та цілісність електронних даних під час доступу до інформаційної системи.

Методи ідентифікації можна поділити на однофакторні та двофакторні. В цьому полягає її схожість з автентифікацією, де також наявні одно та двофакторні методи і вони є еквівалентними тим, що зазначені у ідентифікації. Однофакторні методи діляться на: логічні (паролі, ключові фрази); ідентифікаційні (носієм ключової інформації є безпосередньо об'єкти); біометричні (в їх основі — аналіз унікальних характеристик об'єкту-істоти). Відповідно двофакторними методами є комбінації вищезазначених.

Регламент визначає наступні базові принципи електронної ідентифікації: принцип взаємного визнання; принцип нотифікації схеми електронної ідентифікації; принцип надання гарантій безпеки; принцип інтероперабельності нотифікованих схем електронної ідентифікації; принципи автентифікації; принцип кооперації; принцип відповідальності.

В роботі визначено, що принцип автентифікації є одним з базових принципів електронної ідентифікації, що ще раз підкреслює взаємопов'язаність та необхідність використання ідентифікації разом з автентифікацією. При цьому автентифікація повинна базуватися на принципах безоплатності надання послуги автентифікації, транскордонності та відсутності дискримінації. Визначено, що країни члени ЄС повинні забезпечити можливість транскордонної онлайн автентифікації на основі електронної ідентифікації.

Проведені дослідження показали, що на сьогодні найбільш поширеним методом ідентифікації особи на території нашої держави є електронний цифровий підпис. Проте пропозиція, що міститься в проекті Регламенту Європейського Парламенту та Ради значно розширює можливості користувачів електронного простору у можливостях обирати механізми реалізації ідентифікації.

УДК 621.396

А.А. Замула
Харьковский национальный университет имени В.Н. Каразина
alexz_@bk.ru

МЕТОД ОПТИМИЗАЦИИ ВЫБОРА ДИСКРЕТНЫХ СЛОЖНЫХ СИГНАЛОВ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МНОГОПОЛЬЗОВАТЕЛЬСКИХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Важными характеристиками телекоммуникационных систем являются помехоустойчивость и скрытность функционирования. Под помехоустойчивостью понимают способность системы противостоять воздействию мощных помех. Скрытность функционирования системы предполагает способность системы функционировать в режиме, затрудняющим обнаружение передаваемых сообщений и оценку их параметров разведывательной аппаратурой злоумышленника. Одним из видов скрытности является информационная скрытность. Такой вид скрытности предполагает целый комплекс мер, методов и средств для затруднения определения злоумышленником самого факта передачи сообщений по каналам связи, содержания передаваемых сообщений и другое. Большое значение при решении задач обеспечения требуемой помехоустойчивости и скрытности функционирования (в том числе, информационной скрытности) имеют исследования, связанные с использованием новых видов сигналов, получивших название: сложных, широкополосных, многомерных и шумоподобных. Предпочтительными, являются сигналы с наименьшим значением максимального бокового лепестка функций авто — и взаимной корреляции. Требования, предъявляемые к наилучшему сигналу, могут быть сформулированы в виде следующей оптимизационной задачи: на множестве всех возможных сигналов с символами из заранее выбранного алфавита найти сигнал или сигналы с минимальной величиной максимального бокового лепестка корреляционной функции. Данная оптимизационная задача не имеет общего аналитического решения и процедурой ее выполнения является осуществление исчерпывающего поиска. Разработка методов, оптимизирующих синтез сложных сигналов с необходимыми корреляционными, ансамблевыми, статистическими, структурными и другими свойствами, является актуальной задачей.

Предлагается метод синтеза дискретных сигналов, с использованием которого появляется возможность отказаться от поиска, основанного на переборе всех возможных вариантов для выбора сигналов с необходимыми корреляционными, ансамблевыми, статистическими и структурными свойствами. В качестве источника сложных дискретных сигналов предлагается использовать ключевые последовательности криптографических алгоритмов. В ходе выбора дискретных сигналов производится оценка статистических свойств формируемых дискретных сигналов с использованием известных статистических тестов, оценка соответствия значений боковых лепестков различных функций авто- и взаимной корреляции сигналов-претендентов известным оптимальным границам для

данных функций. Разработанные в ходе исследований теоретические положения позволяют существенно сократить процедуру выбора из множества возможных дискретных сигналов таких, которые удовлетворят критериям оптимальности.

Достоверность разработанных теоретических положений подтверждена средствами программного моделирования.

УДК 621.396

А.А. Замула, Е.А. Семенко

Харьковский национальный университет им. В.Н. Каразина,

semenkoe@gmail.com

ПРОГРАММНЫЙ КОМПЛЕКС ГЕНЕРАЦИИ И ИССЛЕДОВАНИЯ ДИСКРЕТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ПРИЛОЖЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

В телекоммуникационных системах широкое применение получили дискретно-кодированные сигналы (ДКС), в которых манипулируемые параметры (амплитуда, фаза, частота) изменяются через строго фиксированные интервалы времени. Закон применения манипулируемого параметра в ДСК задается дискретными последовательностями (ДП), которые полностью определяют свойства ДКС и часто отождествляются с ними. Поэтому внимание исследователей телекоммуникационных систем оказалось сфокусированным на анализе, синтезе и обработке ДП с необходимыми свойствами.

Предлагаемый метод синтеза систем дискретных последовательностей включает следующие шаги.

1) Генерация массива псевдослучайных последовательностей символов заданного периода с использованием генератора ключей криптографического алгоритма, например, AES.

2) Тестирование полученных последовательностей с применением критериев и показателей качества генераторов, определенных международными и ведомственными стандартами.

3) Получение матрицы состояний корреляционных функций отдельных псевдослучайных последовательностей и всех возможных пар последовательностей, полученных на первом шаге.

4) Формирование границ «плотной упаковки» для различных корреляционных функций.

5) Обработка матрицы, заключающаяся в том, что осуществляется отбор последовательностей, удовлетворяющих границам «плотной упаковки»

Для реализации данного метода был разработан программный комплекс на языке высокого уровня — Java.

Программа использует стороннюю криптографическую библиотеку для реализации алгоритма симметричного блочного шифрования AES (Rijndael). На первой стадии задают параметры для работы программы: длину генерируемого AES ключа (key_length), период исследуемой последовательности (L), а также допустимые границы максимального бокового пика периодической функции

автокорреляции (ПФАК) для отбора ДП, удовлетворяющей заданной границе (N). Далее, алгоритм работы предполагает генерацию ключа алгоритма AES, после чего проводят обработку полученной последовательности: сгенерированный ключ переводится в битовое представление и записывается в отдельный массив. Поскольку на первом шаге определяют длины последовательностей для исследования, программа переходит к основному циклу исполнения. В дополнительный массив копируются первые L бит ключа (0 — L) из key_length, а затем проводится подсчет количества 0 и 1 для определения «баланса» последовательности. После этого проводится исследование ПФАК и оценка максимального бокового выброса: если максимальный боковой пик превышает допустимую границу (N), эту последовательность не используют в дальнейших исследованиях, увеличивают счетчик итераций цикла и выполняют исследования следующих [1-(L+1)] бит ключа, если же максимальный боковой пик равен или не превышает границу (N), данную последовательность записывают в отдельный массив, увеличивают счетчик цикла и осуществляют дальнейший поиск подходящих последовательностей.

После того, как выполнены исследования всех возможных последовательностей из сгенерированного ключа и записи их в отдельные массивы, приступаем к дальнейшему анализу и обработке. Разработанный программный комплекс позволяет проводить исследования различных корреляционных функций ДП.

УДК 004.056

А. Затарі

Державний університет телекомунікацій, kefir06@tambler.ru

ПРОМИСЛОВЕ ШПИГУНСТВО

Промислове шпигунство — це форма несумлінної конкуренції, при якому отримання, використання, розголошення конфіденційної інформації відбувається незаконним шляхом і з метою отримання переваг і, як наслідок, матеріальної вигоди. Промислове шпигунство ведеться на всіх рівнях.

Ним займаються держави, міжнародні організації, окремі особи. Безсумнівно, промислове шпигунство переживе військовий шпіонаж, якщо останній коли-небудь зникне в результаті дійсного роззброєння або здачі всіх видів зброї Організації Об'єднаних Націй.

Стверджують, ніби існують навіть біржі спеціалізованих секретів, де купується і продається крадена технічна інформація; ніби така біржа, що спеціалізується на електроніці і пластичних матеріалах, існує в Японії; інша біржа, яка спеціалізується на виробах фармацевтичної промисловості, знаходиться в Італії.

Таким чином, промислове шпигунство все більше перетворюється на важливе соціальне явище, що заслуговує вивчення. Зрозуміло, серйозно вивчаючи промислове шпигунство, необхідно враховувати і його політичне значення.

Промислові шпигуни використовують будь-які засоби: тут і застосування новітніх досягнень електроніки, і безпосереднє таємне спостереження, і крадіжки зі зломом, і шантаж. Мова йде про справжню таємній війні — настільки ж поширеною і настільки ж незвичайною, як боротьба військових розвідників і контррозвідників.

Методи промислового шпигунства:

1. Підкуп посадової особи, яка має доступ до охоронюваної законом таємниці конкуруючої компанії, з метою отримання даної конфіденційної інформації;

2. Шантаж осіб, зазначених у пункті 1. Так само шантаж може бути об'єднаний з підкупом. Наприклад, коли співробітника просять продати нічого не значущу інформацію, а потім, після успішного завершення даного етапу шантажують фактом продажу, щоб роздобути щось більш значуще;

3. Впровадження агента (або шкідливого програмного забезпечення) в компанію з метою отримання конфіденційної інформації або охороняється законом таємниці;

4. Незаконний доступ до засобів зв'язку і передачі інформації з метою отримання конфіденційної інформації або охороняється законом таємниці;

5. Саботаж компанії або її ресурсів (в тому числі і електронного характеру шляхом DDoS-атак) з метою отримати доступ до конфіденційної інформації або використовувати саботаж в подальшому як засіб шантажу.

Тобто, на основі методів промислового шпигунства можна виділити наступні заходи протидії необхідні для захисту інформації:

1. Проведення ефективної кадрової політики. Зокрема, проводити перевірку минулого, людських якостей претендента, щоб виключити появу всередині компанії потенційних зловмисників;

2. Проведення належного інструктажу і регулярних перевірок. Інструктаж необхідний щоб персонал компанії знав яка інформація є конфіденційною, а який можна ділитися без загроз для безпеки компанії. Перевірки ж дозволять закріпити отриману персоналом інформацію та виявити тих, хто несерйозно або недобросовісно ставиться до питань інформаційної безпеки;

3. Створення позитивної мотивації працівників. Людина, яка чимось незадоволений у своїй роботі — потенційний розповсюджувач конфіденційної інформації про компанію. Він може почати її розповідати навіть випадковому знайомому за барною стійкою тільки для того, щоб виговоритися. Якщо ж йому запропонувати за розголошення винагороду, то подібний співробітник не вагаючись видасть всі відомі йому секрети і таємниці;

4. Створення надійної технічно захищеної бази зберігання та передачі інформації. Тобто створення системи, яка не буде піддана технічним збоїв і буде в змозі витримати будь-яку хакерську атаку.

УДК 004.621.3:519.816

С.В. Зибін

Державний університет телекомунікацій

ВИМОГИ ДО ЕКСПЕРТНОЇ СППР ПО ЗАБЕЗПЕЧЕННЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Специфічними особливостями вирішення завдання створення системи забезпечення інформаційної безпеки являється: неповнота й невизначеність вихідної інформації про ресурси організації й характерних загрозах; багатокритеріальність завдання, пов'язана з необхідністю обліку великої кількості показників та інформації; наявність як кількісних, так і якісних показників, які необхідно враховувати при розв'язанні завдань розробки й впровадження системи забезпечення інформаційної безпеки [1].

Експертна система підтримки прийняття рішення (СППР) по забезпеченню інформаційної безпеки повинна задовольняти наступним вимогам:

- сгенеровані системою рекомендації можуть використовуватися в якості посібника із створення бази знань; методики формування показників і вимог до системи забезпечення інформаційної безпеки; інструмента оцінки кількісних і якісних показників системи забезпечення інформаційної безпеки; інструмента оцінки стану інформаційної безпеки організації;
- мати властивості універсальності, комплексності, масштабованості, простоти використання, наочності, практичній спрямованості, спроможність до самостійного навчання, функціонування в умовах високої невизначеності вихідної інформації;
- виконувати наступні функції: встановлювати взаємозв'язок між вимогами; одержувати кількісні оцінки; оцінювати стан забезпечення інформаційної безпеки; застосовувати різні методики оцінок; оперативно реагувати на зміни умов функціонування інформаційної організації.

У зв'язку із цим необхідно розробити функціональні вимоги, що представляють собою опис природньою мовою функцій, які повинна виконувати експертна СППР по забезпеченню інформаційної безпеки та включають опис того, як система реагує на вхідні дані і як поводиться в певних ситуаціях [2, 3].

До цих вимог відносяться наступні: ініціація процесу, ідентифікація ресурсів, створення моделі об’єкта, оцінка ресурсів, ініціалізація процесу оцінювання рівня забезпечення інформаційної безпеки, оцінювання рівня забезпечення інформаційної безпеки, можливість переривання, порівняння, оптимізація, рекомендації.

Крім того, до експертної СППР пред'являються не функціональні організаційні вимоги щодо розробки системи та створення супутньої документації, мови програмування та моделювання предметної області, а також повинна містити сервіси безпеки.

Література:

1. Баранов В.Л. Відновлення та оптимізація інформації в системах прийняття рішень /Баранов В.Л., Браіловський М.М., Засядько А.А., Казакова Н.Ф., Хорошко В.О. — К: Вид. ДУІКТ, 2009. — 134 С.

2. Баранов В.Л. Моделювання фізичних процесів в інформаційній безпеці. / Баранов В.Л., Капустян М.В., Костюченко Р.М., Хорошко В.О. — К: Вид. ДУІКТ, 2009. — 175 С.

3. Хорошко В.О., Зибін С.В. Оцінка якості функціонування комплексних систем технічного захисту й систем підтримки ухвалення рішення в їхньому складі. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2 (24), 2012 р. — С. 7-15.

УДК 003.26:004.056

Е.В. Исирова

Харьковский национальный університет имени В.Н. Каразина,

katisa2008@mail.ru

-проф. каф БИСТ ХНУ им. В.Н.Каразина И.Д. Горбенко

БИЗНЕС МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для облегчения бизнес операций сегодня предприятия все чаще становятся зависимыми от IT-технологий, прежде всего от уровня информационной безопасности (ИБ). Это подтверждается особым вниманием Европейского Союза к решению проблем предоставления физическим и юридическим лицам електронных доверительных услуг [1].

В целом использование IT-технологий в бизнес процессах позволяет улучшить такие показатели как: снижение затрат на 21%; повышения качества сервиса на 11%; ускорение выхода на рынок на 5%; доступ к новым знаниям на 13%; повышение капитализации на 12% и др.

Целью настоящего доклада является обоснование и анализ бизнес модели ИБ. В докладе показывается, что для обеспечения надлежащей защиты информационных активов необходимо применять комплексный и системный подход с учетом требований ИБ.

Один из основоположных принципов построения модели ИБ предложен международной ассоциацией ISACA. Модель получила название «Бизнес модель информационной безопасности» (рис.1). Она состоит из 4 статических элементов (Организации, Люди, Технологии, Процессы) и 6 динамических (Культура, Архитектура, Управление, Снабжение и поддержка, Проявления, Человеческий фактор), которые связанны между собой и таким образом дают возможность комплексного и системного подхода к вопросам обеспечения информационной безопасности [2].

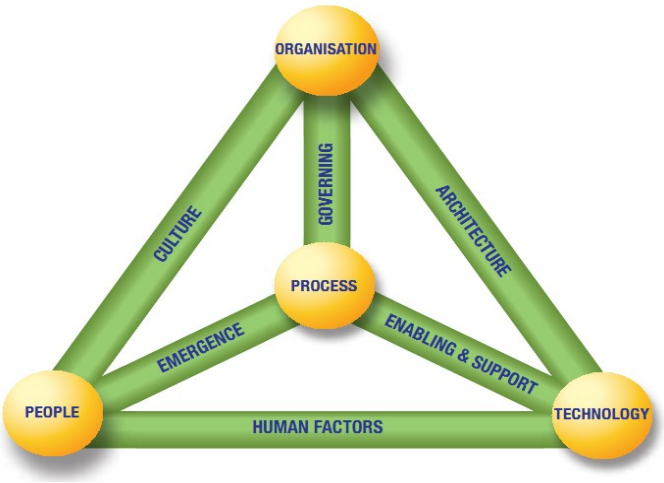


Рис.1- Бизнес модель информационной безопасности

Модель лучше всего рассматривать как гибкую, трехмерную, пирамидальную структуру. Все аспекты модели взаимодействуют друг с другом. Если изменить либо пренебречь, одной из частей, то равновесие модели становиться потенциально под угрозой. Динамические взаимосвязи выступают в качестве индикаторов напреженности, оказывая эффект «Тяни / Толкай» в ответ на изменения на предприятии, что позволяет модели, быть адаптивной по мере необходимости [2]. Преимущества такой модели: 1. Проактивность и взаимосвязь элементов. 2. Комплексность и динамичность. 3. Системность. 4. Повышение эффективности элементов системы. 5. Представляет собой актив и формирует ценность бизнеса.

В целом, применение рассмотренной модели на практике позволяет минимизировать убытки и оперативно влиять на возможные угрозы ИБ.

Список использованных источников:

1. ISACA An Introduction to the Business Model for Information Security-20092. Marco Melo Raposo. Business Model for Information Security -2011

УДК 003.26 (075.8)

А.Г. Карпов

Харківський національний університет імені В.Н.Каразіна

andrey.karpov1994@gmail.com

-проф. каф БІСТ ХНУ ім.. В.Н.Каразіна І.Д. Горбенко

КВАНТОВИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ

Випадкові числа широко використовуються в багатьох галузях науки і технологій, таких як статистичний аналіз, комп'ютерне моделювання, криптографія. Однак в криптографії до випадкових послідовносте висуваються жорсткі вимоги в частині необоротності, непередбачуваності, нерозрізнюваності та складності генерування. Одним з таких джерел випадкових послідовностей є квантовий генератор випадкових чисел. Такий генератор, як показали попередні дослідження, у найбільшій мірі може задовольнити вказаним вище жорстким вимогам. Пропонується декілька основних методів, перевага та порівняння яких не визначена тощо. *Метою цієї доповіді є обґрунтування та вибір критеріїв порівняння та попереднє*

порівняння з їх використанням найбільш відомих методів.

Серед відомих методів необхідно виділити два основних — алгоритмічний і апаратний. Алгоритмічні генератори випадкових чисел не дозволяють отримувати випадкові (детерміновані) числа, які відповідали б жорстким вимогам зі сторони криптографії. В більшості випадків в криптографії необхідно використовувати істинно випадкові числа, що отримані за допомогою фізичних не детермінованих процесів. Ряд переваг перед алгоритмічними генераторами мають генератори, що ґрунтуються на випадковості квантових процесів. Такі процеси обумовлені законами квантової фізики, тому заслуговують уваги та подальшого дослідження.

Визначено, що в якості фізичних явищ при створенні квантових генераторів можна використовувати такі.

1. Дробовий шум — це шум в електричних ланцюгах, що викликаний дискретністю носіїв електричного заряду, шум у оптичних пристроях. Як джерело шуму використовують фотоелектронний помножувач або електровакуумні фотоелементи.

2. Радіоактивний розпад для якого характерна випадковість забезпечується за допомогою кожного окремого акту розпаду. В результаті на приймач в різні проміжки часу потрапляє різна кількість частинок.

3. Спонтанне параметричне розсіяння, яке також може бути використано в генераторах випадкових чисел.

В доповіді обґрунтовується вибір та наводяться результати досліджень генератора випадкових чисел з використанням форм оптичних імпульсів. Такий генератор забезпечує генерування випадкових послідовностей з високою швидкодією (не менше 110 мбіт/сек) та доброю нерозрізнюваністю. Перевірка нерозрізнюваності здійснювалась з використанням методик, що викладені в NIST 800 — 22 2009 та FIPS 140. Таким чином генератор на основі форм оптичних імпульсів є перспективним і може застосовуватись в криптографії.

УДК 621.396.5

О.С. Ковтун, М.В. Гончаренко, І.С. Щербина, доц.

Державний університет телекомунікацій

ЗАСТОСУВАННЯ ТЕОРІЇ ПРИЙНЯТТЯ РІШЕНЬ ПРИ УПРАВЛІННЯ ІНФОКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

Для інфокомунікаційних мереж (ІМ) нового покоління характерне сполучення принципів децентралізованого управління й децентралізованого функціонування окремих елементів. Якщо комп'ютер стає головним елементом користувача мереж наступного покоління, то природно використовувати комп'ютери як інтелектуальні пристрої в різних вузлах мережі й створювати на основі мікропроцесорів окреме встаткування.

Таким чином, ІМ можна розглядати як це мережі розподіленого машинного інтелекту. Вибір між централізованим і розподіленим (децентралізованим) принципами управління системами в багатьох випадках

складний. Але одне можна затверджувати виразно: розподілені системи більш стабільні й здатні деякою мірою коректувати збої в мережі.

Наприклад, якщо керуючий зв'язок буде ушкоджена, вилучений інтелектуальний модуль може продовжувати функціонувати відповідно до останніх отриманих команд. Друга перевага систем розподіленого інтелекту вони здатні гнучко підбудовуватися до змін навколишнього середовища.

Розподілені системи можна розділити на статичні і динамічні. Динамічні властивості розподілених систем визначаються як характеристиками окремих підсистем, так і характеристиками їх зв’язків. Якщо стан підсистеми залежить лише від її параметрів та зовнішніх впливів, то така підсистема є статичною. Якщо стан підсистеми залежить також від попередніх станів, то така підсистема є динамічною. Розподілена система може бути динамічною (РДС) навіть якщо вона складається із статичних підсистем. Якщо вплив на підсистему з боку інших підсистем залежить від їх попередніх станів через затримку у розповсюдженні впливу між підсистемами, то така динамічна система може мати динамічні властивості.

В загальному випадку задачу прийняття рішень формулюють як задачу вибору найкращого в деякому сенсі рішення з множини допустимих рішень. На практиці розв’язання задач прийняття рішень є досить складною, що обумовлено невизначеністю ситуації, в якій приймається рішення. Для оцінки наслідків від прийняття рішення використовуються втрати, які може понести особа, яка приймає рішення, через відсутність повної інформації про ситуацію прийняття рішення. В залежності від ступеня невизначеності виділяють задачі прийняття рішень в умовах невизначеності, коли про ситуацію прийняття рішень невідомо нічого, крім можливої множини станів, і задачі прийняття рішень в умовах ризику, в яких відомі ймовірнісні характеристики впливів на об’єкт управління. Головний крок в процесі прийняття рішень полягає в перетворенні функції втрат у функцію ризику, яка є функцією двох аргументів: ситуації та рішення.

Ефективність прийнятого рішення залежить від кількості та достовірності використаної інформації. Чим більший обсяг достовірних даних, тим вища ефективність прийнятого рішення. Проте в розподілених системах, що працюють в реальному масштабі часу, буває досить складно забезпечити високу достовірність всіх вхідних параметрів. Це пов’язано з неодночасністю вимірювань в різних точках розподіленої системи, витратами часу на збір даних. В результаті процес прийняття рішення відбувається через деякий час після вимірювання, за який стан системи може відхилитися від виміряного значення.

УДК 159.92.07

К. В. Кравченко

Київський національний університет імені Тараса Шевченка, kvkden@ukr.net

ПРО ІНФОРМАЦІЙНУ БЕЗПЕКУ ОСОБИСТОСТІ

Останнім часом, як ніколи раніше, досить гостро постало питання захисту не лише матеріальних, а й духовних потреб у ресурсах і технологіях, у взаєминах із іншими, в інформації та моральних ідеалах, необхідних для

життєзабезпечення та розвитку особистості. Це зумовлено тим, що збільшилась кількість дестабілізуючих, дезорієнтуючих, дезінформуючих, тиснучих, руйнівних та ін. інформаційних впливів на особистість через:

- засоби масової інформації (радіо, пресу, телебачення), агітаційно-пропагандистські засоби (відеокасети, електронні підручники та енциклопедії тощо);
- психотронні засоби (спеціальна відеографічна та телевізійна інформація, відеозасоби нових інформаційних технологій типу «віртуальна реальність» тощо);
- електронні засоби (оптико- та радіоелектронні засоби, тобто спеціальні передающие устройства та випромінювачі електромагнітних хвиль та імпульсів тощо, електронно-обчислювальні засоби, а саме: «комп'ютерні віруси», що руйнують програмні «закладки-черви» тощо);
- лінгвістичні засоби (мовні одиниці, спеціальна термінологія, обороти мови, що мають семантичну неоднозначність при перекладі на інші мови та ін.);
- психотропні засоби (спеціально-структуровані ліки, транквілізатори, психофармакологічні та психодислептичні засоби, алкоголь, антидепресанти, галюціогени, наркотики тощо).

Саме тому слід здійснювати пошук шляхів і засобів, які б сприяли інформаційній безпеці особистості, тобто стану, який забезпечує особистості можливість об'єктивно оцінювати обстановку, приймати вірні рішення на основі сучасної та достовірної інформації. Це, в свою чергу, буде сприяти зниженню проявів агресії, недовіри один до одного, відчуття психологічного неблагополуччя, неадекватної самооцінки; унеможливлюватиме появу злобних висловів, хамської поведінки, тролів (людина-анонім, яка гуляє по сайтах, форумах і щоденниках, пише провокаційні коментарі тощо), а також мінімізуватиме негативні переживання, страхи, невпевненість у собі, безкультур'я [2-3].

Не втратити індивідуальну унікальність, сенс життя та ін. можна, зокрема, через формування новоутворень психічних якостей особистості. До складу новоутворень належать не лише сукупність знань, умінь та навичок, отриманих і сформованих особистістю під час адаптації, а й складна система міжособистісної взаємодії з оточуючими (родина, друзі тощо) [1]. Корегуючи свою внутрішню систему образів зовнішнього світу, особистість зможе вижити та жити у сучасному світі та зберегти себе як особистість, свої значимі цінності, мати власний погляд на світ, робити власний вибір, самій визначати своє місце у житті.

Список використаних джерел:

1. Дружилов С. А. Психология выживания личности /С. А. Дружилов // Успехи современного естествознания. — 2012. — № 11 (2). — С. 54-57.

2. Зотова О. Ю. Социально-психологическая безопасность личности : Автореф. дис… д-ра психол. н. /19.00.05 — социальная психология /О. Ю. Зотова. — М., 2011. — 43 с.

3. Серебряков В. В. Новая модель безопасности : диалектика средств ее обеспечения / В. В. Серебряков // Мировая экономика и мировые отношения. — 1991. — № 3. — С. 31-40.

4. Куликов Л. В. Психогигиена личности. Вопросы психологической устойчивости и психопрофилактики: учеб. пособие /Л. В. Куликов. — СПб.: Питер, 2004. — 464 с.

УДК 621.396

В.В. Курдеча, М.А. Чирченкова

НТУУ «КПІ», vasyl_kurdecha@mail.ru, chirchenkova.mariya@gmail.com

ЗАЩИТА SDR-ТЕРМИНАЛА ОТ ВОЗДЕЙСТВИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

На сегодняшний день технология Software Defined Radio (SDR) развивается достаточно динамично и является одним из средств перехода к гибким мультистандартным реконфигурируемым сетям.[1] В связи с этим, возникли специфические для SDR проблемы безопасности. Такими проблемами являются: 1)изменение или уничтожение конфигурационных данных; 2)изменение или уничтожения программного обеспечения операционной системы реального времени; 3)изменение или уничтожение данных пользователей; 4)изменение или уничтожение программного фреймворка; 5)изменение или уничтожение кода сигнала; 6)искусственное потребление ресурсов и т.д.

Проблемы 1-6 могут быть вызваны установкой вредоносного программного обеспечения, что делает систему SDR более уязвимой, по сравнению с традиционными телекоммуникационными системами.[2] Поэтому возникает потребность в поиске оптимального метода защиты SDR-терминалов от вредоносного программного обеспечения.

Для обеспечения программной безопасности SDR-терминалов необходимо обеспечение надежного механизма загрузки программного обеспечения из разных источников и создание безопасной среды исполнения программ в терминале.[2]

Предложен метод обеспечения выполнения высоконадежного ПО с предварительным запуском нового компонента в защищенной среде (так называемой «песочнице»), где компонент может быть оценен без ущерба для реальной системы. В таком случае защита от вредоносного ПО и наблюдение за памятью может дополняться мониторингом радиоизлучения. При этом используется два вида обнаружения вредоносного ПО: обнаружения на основе подписей и обнаружение на основе поведения.

Необходимо условно разделить ПО, использующее SDR-терминалы на пользовательское ПО и ПО, обеспечивающее SDR-функциональность терминала. Для уменьшения потенциального количества вычислений терминала в случае запуска в «песочнице» как пользовательского ПО, так и ПО, обеспечивающее SDR-функциональность терминала, разделим обязанности защиты от вредоносного ПО между терминалом и когнитивной системой

управления сетью. В таком случае пользовательское ПО запускается в «песочнице» абонентским терминалом, а ПО, обеспечивающее SDR — функциональность терминала, — средствами когнитивной системы управления сетью.

Ответственным за запуск SDR-функционального ПО в «песочнице» является менеджер абонентского ПО. Он осуществляет хранение, запуск в «песочнице» программных компонентов абонентских терминалов и их учет.

Выводы: В работе был предложен метод защиты SDR — терминалов от вредоносного ПО с помощью распределения запуска в «песочнице» ПО терминалом и менеджером абонентского ПО.

Список использованной литературы:

1. Глоба Л.С., Курдеча В.В., Зингаева Н.А. «Использование SDR-решений в реконфигурируемых мобильных сетях» — Наукові записки УНДІЗ, 2011.

2. BALDINI *et al.*: Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead — IEEE communications surveys & tutorials, vol. 14, no. 2, second quarter 2012

L. B. Michael, M. J. Mihaljevic, S. Haruyama, and R. Kohno, «A framework for secure download for software-defined radio», *IEEE Commun. Mag.*, July 2002.

УДК 004.056

О.А. Курченко, к.т.н., с.н.с., О.А. Халапсіна

Державний університет телекомунікацій

ТЕХНІЧНІ ЗАХОДИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Для реалізації ефективних заходів щодо захисту інформації потрібна не тільки розробка засобів захисту інформації в мережі і розробка механізмів моделі захисту інформації, а і реалізація системного підходу або комплексу захисту інформації. Комплекс захисту інформації, як правило, використовує спеціальні технічні та програмні засоби для організації заходів захисту інформації.

Розрізняють п'ять основних засобів захисту інформації — технічні; програмні; криптографічні; організаційні; законодавчі.

На сьогоднішній момент існує велика кількість технічних рішень у сфері забезпечення інформаційної безпеки. *До технічних заходів належать*:

- міжмережеві екрани (Firewall) від різних виробників як «залізні», так і у вигляді програм, що встановлюються на сервери,
- антивірусні програми,
- системи запобігання витоків даних (Data Loss Prevention Systems),
- системи запобігання вторгнень (Intrusion Prevention Systems) ,
- системи резервного копіювання і відновлення інформації,

- системи відеоспостереження, системи контролю доступу в приміщення.

Всі ці рішення мають великий розкид цін і різні функціональні можливості. Вибір конкретних рішень повинен бути заснований на ризик-аналізі.

Проблеми інформаційної безпеки у сфері технічного захисту інформації:

- Перехоплення електронних випромінювань — проблема вирішується забезпеченням захисту інформації, яка передається по радіоканалах зв'язку та обміну даними інформаційної системи;
- Примусове електромагнітне опромінення (підсвічування) ліній зв'язку з метою отримання паразитної модуляції — проблема вирішується за допомогою інженерного або фізичного захисту інформації. Сюди також відноситься захист інформації в локальних мережах, в інтернеті і технічні засоби інформаційної безпеки:
- Застосування підслуховуючих пристроїв;
- Копіювання носіїв інформації з подоланням заходів захисту;
- Маскування під зареєстрованого користувача;
- Маскування під запити системи;
- Використання програмних пасток;
- Використання недоліків мов програмування і операційних систем;
- Незаконне підключення до апаратури та ліній зв'язку спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;
- Зловмисне виведення з ладу механізмів захисту;
- Розшифрування спеціальними програмами зашифрованої інформації;
- Інформаційні інфекції.

Для запобігання вищеперелічених шляхів витоку інформації за оцінкою інформаційної безпеки необхідний високий рівень технічних знань, крім цього потрібно володіти високим рівнем знань апаратних і програмних засобів захисту інформації. Тому для захисту інформації потрібен комплексний підхід, що включає використання описаних засобів і вимагає дотримання політики безпеки на всіх рівнях діяльності підприємства.

Список використаних джерел:

1) А.А. Садердинов, В.А. Трайнёв, А.А. Федулов «Информационная безопасность предприятия» ИТК Дашков и К, 2005. — 336 с.

2) www.ik.3dscorpion.com.ua

3) www.factor-ltd.by

УДК 621.391.54

М.В. Кутовий, В.П. Новіков, проф.

Державний університет телекомунікацій

МОДЕЛЬ СИСТЕМИ МЕНЕДЖМЕНТУ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В сучасних умовах жоден комплекс програмно-технічних засобів, що підтримується відповідним штатом фахівців з інформаційної безпеки не здатний забезпечити ефективне функціонування системи захисту інформації. Дане питання вимагає системного підходу та розробки комплексних систем управління безпекою, в яких мають брати безпосередню участь всі співробітники організації. Задачами системи управління інформаційною безпекою є систематизація процесів забезпечення захисту інформації, розташування пріоритетів організації в галузі захисту інформації, забезпечення адекватності системи існуючим ризикам тощо.

В роботі сучасних систем моніторингу інцидентів виділяються наступні етапи: визначення інциденту; сповіщення про виникнення інциденту; реєстрація інциденту; усунення наслідків і причин інциденту; розслідування інциденту; реалізація дій, що застерігають повторне виникнення інциденту.

Необхідно відзначити, що система управління інцидентами інформаційної безпеки є базовою частиною загальної системи управління інформаційною безпекою і дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, що адекватний сучасним стандартам і галузевим нормам. Для найбільш ефективної реалізації системи управління інцидентами інформаційної безпеки необхідно спиратись на вимоги міжнародних і галузевих стандартів, таких як ISO\IEC 27001-2013 "Information security management systems. Requirements" та ITU-T X-1051 "Information security management systems. Requirements for telecommunications".

Управління інцидентами, це важливий процес, який забезпечує організації можливість спочатку виявити інцидент, а потім за допомогою коректно обраних засобів підтримки якомога швидше його вирішити.

Основне завдання управління інцидентами — якомога швидше відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на роботу організації для підтримки якості і доступності служб на максимально можливому рівні. Нормальною вважається робота служб, що не виходить за рамки угоди про рівень обслуговування.

Цілі управління інцидентами:

- відновлення нормальної роботи служб в найкоротші терміни;
- зведення до мінімуму впливу інцидентів на роботу організації;
- забезпечення злагодженої обробки всіх інцидентів і запитів обслуговування;
- зосередження ресурсів підтримки на найбільш важливіших напрямах;
- надання відомостей, що дозволяють оптимізувати процеси підтримки, зменшити кількість інцидентів і зпланувати управління.

Для захисту від кібератак кожна компанія намагається застосовувати найбільш ефективні та продуктивні системи і моделі захисту інформаційних ресурсів та управління їх безпекою. Основним завданням систем управління, які, серед іншого, забезпечують цілісність даних в організації, є своєчасне та оперативне реагування на кібератаки (кіберзагрози) в інформаційно-комунікаційних системах (ІКС), виявлення та уникнення рецидиву інцидентів, визначення шляхів усунення їх наслідків і розробка превентивних заходів. Як показав аналіз, універсальної системи, яка б задовольняла усім вимогам керівників, враховувала б специфіку ІКС і забезпечувала її безперервну роботу, не існує.

УДК 354.42

О.В. Левченко
кандидат військових наук, професор
Міністерство оборони України,
alexlev2000@ukr.net

МЕТОДИЧНИЙ ПІДХІД ДО ПРОВЕДЕННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

У зв'язку з невпинним зростанням ролі і значення інформації у воєнній справі та стрімкими змінами у сфері інформаційних технологій, воєнно-політичне керівництво провідних країн світу посилену увагу приділяє удосконаленню підходів до організації і ведення інформаційних операцій. Вважається, що метою інформаційних операцій (далі — ІО) є створення сприятливих умов для успішного проведення наземних операцій і бойових дій, ефективного застосування своїх військ, а також зниження ефективності застосування військ противника шляхом захоплення і утримання інформаційної переваги над ним під час підготовки і в ході воєнних дій. Тому дослідження шляхів підвищення ефективності ІО є **нагальною науковою проблемою.**

Особливо важливим є пошук дієвих механізмів проведення ІО в умовах російської агресії проти України в Криму та на Сході нашої Держави, що і визначає **актуальність цього дослідження**.

Таким чином, **метою статті** є розроблення методичного підходу до проведення інформаційних операцій.

За поглядами іноземних військових фахівців ІО завжди повинні розпочинатися заздалегідь до початку операцій угруповань військ, адже за умови цілеспрямованої підготовки і якісного проведення така операція може не лише суттєво вплинути на розвиток воєнного конфлікту, а і призвести до припинення його ескалації, не даючи йому перерости у збройне протистояння. Важливо, що ІО повинні вестися не тільки впродовж операцій угруповань військ для забезпечення сприятливих умов виконання визначених їм завдань, а і продовжуватися після їх завершения для створення умов щодо закріплення їх результатів.

Для найбільшої результативності ІО пропонується методику її планування і проведення здійснювати за такими етапами.

Підготовчий етап. Сутність цього етапу полягає у плануванні операції, визначенні сил і засобів, що залучаються, та їх підготовці до проведення заходів інформаційного впливу.

Початковий етап. На етапі обирається або штучно створюється так званий інформаційний привід — це подія, якою можна скористатися як приводом для розгортання скоординованих інформаційно-психологічних акцій. Як інформаційний привід може бути використана будь-яка подія, яка якимось чином співвідноситься з наявними проблемами, актуальними стереотипами і викликає живий інтерес у визначеної аудиторії (об'єкта впливу).

Основний етап. Це є найбільш складний і достатньо тривалий етап операції. Його сутність полягає у масованому і повному використанні залучених інформаційних ресурсів для формування або руйнування визначених психологічних стереотипів і установок у об'єктів, на які спрямовується вплив. Фактично цей етап є сукупністю інформаційних заходів, пропагандистських і психологічних акцій та інших дій, які проводяться за єдиним замислом для досягнення поставленої мети операції.

Заключний етап. Зміст цього етапу полягає у плавному завершенні інформаційної операції та закріпленні її результатів після досягнення поставлених цілей операції чи в результаті якихось форс-мажорних обставин. Головне завдання етапу — вийти з операції таким чином, щоб супротивник навіть не здогадався про її проведення, або хоча б не дати можливості йому зрозуміти мети проведеного на нього впливу.

Висновок. Застосування запропонованого методичного підходу, заснованого на наведених вище етапах, дозволить більш повно і завчасно готувати та більш ефективно проводити інформаційні операції.

УДК 004.056.5

Н.В. Лукова-Чуйко, к.ф-м.н.

Київський національний університет імені Тараса Шевченка, lukova@ukr.net

МОДЕЛЮВАННЯ ОПТИМАЛЬНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Сучасні системи захисту інформації являють собою складні структури, які можуть містити велику кількість об'єктів захисту. Дослідження таких систем представляє складну задачу, яку розглядають зазвичай з допомогою математичної моделі. Це абстрактний образ реальної фізичної системи, котрий повинен відповідати двом суперечливим величинам: в найбільшій степені відображати властивості системи, уникаючи при цьому зайвої деталізації, яка може ускладнити одержання кінцевих результатів. Інтерес до математичного моделювання в сфері інформаційної безпеки зростає з часом з огляду на збільшення обсягів і цінності інформації, масовості нападів, розширення і вдосконалення засобів отримання несанкціонованого доступу до інформації та засобів захисту інформації; збільшення вартості інформації. Ускладнення

систем відбивається на структурі математичних моделей, які повинні відображати нові умови і виникаючі ситуації.

Основним завданням менеджменту інформаційної безпеки є оптимізація її технічних і економічних показників. До основних завдань менеджменту інформаційної безпеки належить оптимізація використання інвестицій у захист інформації. Цей напрямок має декілька аспектів, в яких оптимізації підлягають:

- загальна кількість інвестицій у захист;
- їх розподіл між окремими об'єктами;
- момент інвестування.

Критерієм оптимальності може бути один або декілька показників інформаційної безпеки — величина завданої шкоди від реалізації загроз інформації, загальні витрати, які включають збиток від витоку інформації і витрати на її захист; прибуток від внесення інвестицій в захист інформації, їх рентабельність тощо.

Рішення поставлених задач ускладнюється низкою причин. Головна з них обумовлена тим, що пошук оптимального рішення ведеться в умовах невизначеності, коли дії суперника можна передбачити лише з певною імовірністю, а іноді взагалі неможливо. Різноманітність засобів та засобів захисту, їх характеристик, різноманітність каналів несанкціонаваного отримання інформації, уразливість окремих елементів системи захисту.

Рішення задачі оптимізації використання інвестицій для широкого класу систем інформаційної безпеки дає можливість покращити економічні і технічні показники.

Побудову математичної моделі поділено на декілька етапів.

▪ Обрати показник, який визначає цільову функцію і підлягає оптимізації. Такими показниками можуть бути: надійність системи, збиток від витоку інформації, розмір інвестицій у захист інформації, їх рентабельність, сумарні втрати, що включають збиток від витоку інформації і витрати на її захист тощо.

▪ Визначити параметри і характеристики системи, від яких залежить цільова функція.

▪ Зібрати відомості про систему захисту (модель загроз та модель порушника).

▪ Встановити вид залежності цільової функції від параметрів і характеристик системи захисту.

▪ Обрати критерій оптимальності (збиток від витоку інформації, максимально допустиме значення для кожного з об'єктів).

Організація розрахунків передбачає операції:

- вибір методу розв'язку задачі;
- складання і налагодження програми для комп'ютера;
- проведення розрахунків;
- представлення результатів у найбільш виразній формі;
- формулювання висновків і рекомендацій.

УДК 621.376.54

М.К. Майстренко

Державний університет телекомунікацій

СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ КАРТКОВИХ РОЗРАХУНКІВ

На думку експертів, міжнародні платіжні системи, такі як VISA International, MasterCard WorldWide, строго регламентують технології випуску пластикових карток. Відповідно, вони досконально прописують всі елементи захисту при виготовленні карток. Окремі з них дублюють норми виробництва паперових грошей — наприклад, елементи, що світяться; якщо взяти картку і покласти під лампу, то можна побачити певні знаки. Крім того, дані регламенти та маркування на картці дозволяють досить точно визначити, коли і ким вона була випущена. Люди, які займаються випуском контрафактної продукції, навряд чи знають про такі нюанси.

Кожна картка після стадії виробництва проходить процедуру затвердження в платіжній системі. Це також є певним ступенем захисту. Банк завжди замовляє точну кількість карток, що друкується на картковому заводі. Після цього банк звітує за весь тираж в платіжну систему.

На сучасних карткових заводах використовуються спеціальні фарби для забезпечення високого ступеня захисту банківських карток. Тільки підприємство, сертифіковане на випуск банківських карток, знає тонкощі виробництва таких карток (шрифт, кегль, світність фарби та інші графічні можливості).

Постійно ведуться розробки нових систем IT-безпеки. Таких розробок чимало. Але вся складність полягає у тому, що галузь інформаційної безпеки досить жорстко регламентується. Існують нормативні акти, що описують вимоги до систем захисту, а також вимоги до їхньої оцінки відповідності. Нові системи повинні відповідати цим вимогам, що дуже непросто; це змушує банки або застосовувати несертифіковані засоби захисту, або не використовувати їх зовсім.

Але основна проблема в іншому — багато компаній не використовують навіть існуючі засоби безпеки, що добре себе зарекомендували, не кажучи вже про новинки.

Постійне вдосконалення методів та інструментів, якими користуються кіберзлочинці, призводить до необхідності створювати нові системи інформаційної безпеки. Сьогодні розробники таких рішень вже відмовилися від так званого «принципу замка», який базувався виключно на ідеї «не пускати». Практика показала, що найбільш ефективний метод полягає не в стримуванні, а в реалізації активного відгуку на загрозу інформаційній безпеці.

Створення таких систем є пріоритетним завданням у сфері захисту інформації. Такі продукти будуть не тільки детектувати порушення та припиняти його, але й автоматично здійснювати збір цифрових доказів. Ці дані дозволять правоохоронним органам оперативно виявити зловмисників та притягнути їх до відповідальності. Подібні технічні засоби сприятимуть не лише захисту інформації, а безпосередньо допоможуть знизити сам рівень кіберзлочинності.

УДК 004.056.53

В.В. Мохор, д.т.н., професор, В.В. Цуркан, к.т.н., О.М. Крук
Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ»,
v.v.tsurkan@gmail.com
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України,
onk@conferen.ru

НОРМАТИВНО-ПРАВОВИЙ АСПЕКТ РОЗРОБЛЯННЯ СИСТЕМИ МЕНЕДЖОВУВАННЯ РИЗИКУ БЕЗПЕКИ ІНФОРМАЦІЇ

Конфіденційність, цілісність та доступність інформації забезпечується за результатами оцінювання ризику шляхом прийняття рішень про необхідність його обробляння [1, 3]. Для цього рекомендується розробляти систему менеджовування ризику безпеки інформації. Загальні принципи та рекомендації її побудови викладаються в міжнародних стандартах серій 27k і 31k [1 — 4], а саме: ISO/IEC Guide 51:2014, ISO/IEC 27000:2014, ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27005:2011, ISO Guide 73:2009, ISO 31000:2009, ISO/IEC 31010:2009, ISO/TR 31004:2013. З огляду на це, розгляд нормативно-правового аспекту розробляння означеної системи вважається актуальним.

У міжнародних стандартах ISO/IEC 27001:2013 та ISO/IEC 27002:2013 розкривається доцільність визначення та впровадження процесів оцінювання та обробляння ризику. Взаємопов'язаність означених процесів забезпечується встановленням критеріїв прийняття та оцінювання ризику; гарантуванням можливості отримання логічних, обґрунтованих та зіставних оцінок; обранням варіанту обробляння ризику, засобами та заходами реалізації варіанту обробляння ризику; розробленням положення про прийняття ризику; розробленням та узгодженням з його власниками відповідного плану обробляння [1, 4].

Терміни, визначення, принципи та рекомендації розробляння системи менеджовування ризику безпеки інформації викладено в міжнародних стандартах ISO/IEC Guide 51:2014, ISO/IEC 27000:2014, ISO Guide 73:2009, ISO 31000:2009, ISO/TR 31004:2013 та ISO/IEC 27005:2011. Крім цього, в них описано процес менеджовування ризику безпеки інформації за видами дій (визначення контексту; оцінювання ризику; обробляння ризику; прийняття ризику; обмін інформацією про ризик; контролювання та переглядання ризику [2, 3]). Результативність таких дій досягається завдяки, наприклад [3], націленості на захист реальних цінностей; залученості до всіх організаційних процесів; причетності до прийняття рішень; врахуванні всіх невизначеностей; систематичності, структурованості та регулярності дій; актуальності інформації, що використовується. Однак, в означених стандартах розкрито узагальнений підхід до визначення та впровадження процесів оцінювання та обробляння ризику. Тому викладені в них положення доповнюються рекомендаціями міжнародного стандарту ISO/IEC 31010:2009.

Таким чином, розгляд нормативно-правового аспекту розробляння системи менеджовування ризику безпеки інформації дозволить визначити призначення та можливості означеної системи, а також встановити перелік її

елементів та взаємозв'язків між ними для забезпечити конфіденційності, цілісності та доступності інформації.

Список використаних джерел:

1. Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013. — [Second edition 2013-10-01]. — Geneva, 2013. — P. 23.

2. Information technology. Security techniques. Information security risk management: ISO/IEC 27005:2011. — [Second edition 2011-06-01]. — Geneva, 2011. — P. 68.

3. Risk management. Principles and guidelines: ISO 31000:2009. — [First edition 2009-11-15]. — Geneva, 2009. — P. 24.

4. Мохор В.В. Спроба локалізації ISO GUIDE 73:2009 «Risk management — Vocabulary» / В.В. Мохор, О.М. Богданов, О.М. Крук, В.В. Цуркан // Безпека інформації. — 2012. — № 2 (18). — С. 12 — 22.

УДК 004.056.53

В.В. Мохор, д.т.н., професор, О.В. Цуркан, Р.П. Герасимов

ДП «Укртехінформ», o-v-c@yandex.ru

Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАНУ, gerasimov.rostislav@gmail.com

СОЦІОІНЖЕНЕРНА ЗАГРОЗА ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІЙ БЕЗПЕЦІ ЛЮДИНИ В КІБЕРПРОТОРІ

Головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає кібернетичний простір. Це обумовлено тим, що сучасні інформаційні технології дають змогу їм реалізувати власні інтереси без застосування військової сили, послабити або завдати значної шкоди безпеці конкурентної держави через відсутність дієвої системи захисту від негативного інформаційно-психологічного впливу. Такий вплив орієнтований на свідомість та підсвідомість людини з метою внесення змін у її поведінку та світогляд. Тому забезпечення інформаційно-психологічної безпеки людини є життєво важливим інтересом держави в кібернетичному просторі [1–3].

Однак, на практиці можливе ускладнення в задоволенні цього інтересу через реалізацію таких загроз як вплив на процес міжособистісної комунікації, використання маніпулятором внутрішніх чинників, використання маніпулятором зовнішніх чинників. Тому негативний інформаційно-психологічний вплив оцінюється з позицій руйнування чи перекручування головних системоутвоюючих якостей людини як цілісність і розвиток. Завдяки цьому визначаються аспекти прояву наслідків такої діяльності, які стосуються системи відносин людини до держави та руйнування цілісності людини [2, 4].

Разом з тим, наведений перелік загроз доцільно доповнити соціоінженерною загрозою, як однією з найбільш небезпечних в кіберпросторі [2]. Її сутність полягає в маніпулятивному впливові на свідомість (підсвідомість) людини через властиві їй вразливості. Зокрема, її слабкості , потреби, манії (пристрасті), захоплення. Маніпулювання ними дозволяє отримати несанкціонований доступ до інформації без руйнування та

перекручування головних для людини системоутвоюючих якостей. При цьому маніпулювання уразливостями людини виражається в таких формах як, наприклад, шахрайство, обман, афера, інтрига, містифікація, провокація. Використанню кожної з них передує ретельне планування та організація [3, 4].

Таким чином, реалізація соціоінженерної загрози орієнтована на отримання несанкціонованого доступу до інформації шляхом маніпулятивного впливу на свідомість або підсвідомість людини проти волі, але за її згодою. В кінцевому випадку це призводить до нової моделі поведінки людини та створення сприятливих обставин реалізації соціоінженерних атак в кіберпросторі.

Список використаних джерел:

1. Про Доктрину інформаційної безпеки України: Указ Президента України від 08.07.2009 № 514/2009 [Електронний ресурс] / Укази // Упр. комп'ютериз. систем Апарату Верховної Ради України. — Режим доступу: http://zakon4.rada.gov.ua/laws/show/514/2009. — Дата доступу: лютий 2014. — Назва з екрану.
2. Мохор В. В. Наставления по кибербезопасности (ISO/IEC 27032:2013) / В. В. Мохор, А. М. Богданов, А. С. Килевой. К.: ООО «Три-К», 2013. — 129 с.
3. Жарков Я.М. Інформаційно-психологічне протиборство (еволюція та сучасність): Монографія / Я.М. Жарков, В.М. Петрик, М.М. Присяжнюк та ін. — К.: ПАТ «Віпол», 2013. — 248 с.
4. Цуркан О.В. Соціоінженерний аспект негативного інформаційно-психологічного впливу на людину в кіберпросторі / О.В. Цуркан, В.В. Мохор // ITSEC: IV міжн. наук.-практ. конф., 20–23 травня 2014 р.: тези доп. — К.: НАУ, 2014. — С. 46.

УДК 004.056.003.12 (083.94)

І.В. Никифорук, О.О. Мелешко

Національний авіаційний університет. Iranuk870@gmail.com

ОЦІНКА ЗБЕРІГАННЯ ДАНИХ В «ХМАРНИХ» СЕРВІСАХ

Cloud-технології швидко розвиваються і знаходять своє місце у всіх сферах діяльності людини. Великі компанії для зменшення витрат обслуговування робочих місць створюють штаби для віддаленої роботи через Інтернет, а користувачі відмовляються від потреби перенесення інформації на з'ємних носіях в користь хмарних обчислень.

Актуальність даної теми полягає в тому, що cloud-системи широко інтегровані, і через це є великий ризик зараження файлів вірусними програмами. Тому виникає питання про цілісність і доступність даних, які знаходяться у провайдера, адже він несе відповідальність за збереження інформації.

На даний момент на ринку «хмарних» послуг надається декілька десятків cloud-сервісів. Найпопулярніші з них:

- Oracle Cloud;

- Google Drive;
- Dropbox;

Так як, на «хмарних» сервісах зберігається інформація різного характеру, і переважно являється конфіденційною, то втрата особистих даних, приведе до критичних наслідків, тому доцільно провести оцінку зберігання інформації на вищеперерахованих cloud-сервісах.

Найважливішою частиною оцінки безпеки зберігання даних на «хмарних» серверах вважається емпіричне дослідження, спрямоване на збір та аналіз даних з оцінками результату використання «хмарних» сховищ даних.

Для виявлення найбільш ефективних хмарних сервісів, в таблиці наведено порівняльний аналіз функціональних можливостей виходячи з функціональних критеріїв.

Табл. 1. Оцінка «хмарних» сервісів.

№ п/п	**Критерії оцінки**	**Google Drive**	**Sky Drive**	**DropBox**
1	Загальна оцінка	69.9	69.1	79.4
2	Функціональність	77	76	96
3	Швидкодія	83	81	63
4	Захист даних	42	42	70
5	Шифрування на стороні клієнта/ при передачі/ на стороні сервера	-/+/-	-/+/-	-/+/+
6	Інтеграція в провідник	+	+	+
7	Додатки для Android\iOS	+/+	+/-	+/+
8	Локальне зберігання	+	+	+
9	Автоматична синхронізація	+	+	+
10	Синхронізація LAN	-	-	+
11	Надання доступу до файлів	+	+	+
12	Інкременте завантаження	-	-	+
13	Паралельне завантаження файлів	-	-	+
14	Історія змін	-	+	+

Провівши оцінку Cloud-сервісів видно, що дані сервери погано направлені на безпеку конфіденційної інформації, так як надається широкий доступ до даних користувачу з будь-яких пристроїв, та операційних систем.

На сьогоднішній день з цілковитою впевненістю не можна сказати, наскільки захищені дані в «хмарних» сховищах, але методи які направлені на забезпечення їхньої безпеки розвиваються.

Науковий керівник — доцент кафедри КСЗІ Мелешко О.О.

УДК 004.056

О.Г. Оксіюк, д.т.н., В.І. Вялкова, к.т.н.

Київський національний університет імені Тараса Шевченка

ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ ОПЕРАЦІЙНОЇ СИСТЕМИ

Операційна система є найважливішим програмним компонентом комп'ютера, тому від рівня реалізації політики безпеки інформації у операційній системі багато в чому залежить і загальна безпека інформаційної системи.

Захищена операційна система повинна мати чітко визначену політику і реалізовувати наступні вимоги.

Політика поширюється на всі об'єкти захищеної операційної системи, що впливають на безпеку інформації.

До таких об'єктів належать:

- адміністратор безпеки та співробітники служби захисту інформації;
- користувачі, яким надані повноваження інших адміністраторів;
- користувачі, яким надано право доступу до інформації, що захищається;
- файли, які містять інформацію, що підлягає захисту;
- програмне забезпечення захищеної операційної системи;
- технологічна інформація механізмів захисту (дані щодо персональних ідентифікаторів та паролів користувачів, їхніх повноважень та прав доступу до об'єктів, інформація журналів реєстрації дій користувачів тощо);
- засоби адміністрування та управління захищеною операційною системою та технологічна інформація, яка при цьому використовується;
- окремі периферійні пристрої, які задіяні у технологічному процесі обробки інформації;
- обчислювальні ресурси, безконтрольне використання яких чи захоплення окремим користувачем може призвести до блокування роботи інших користувачів або захищеної операційної системи в цілому.

Комплекс засобів захисту повинен надавати можливість реалізовувати політику адміністративного керування доступом. Повинна забезпечуватися наявність механізмів рейтингів захисту (міток доступу, списків доступу), що присвоюються об'єктам захисту.

Розмежування інформаційних потоків між користувачем та пасивним об'єктом має відбуватися на основі рейтингу захисту користувача, рейтингу захисту об'єкта та атрибутів доступу користувача та об'єкта.

Список використаної літератури

1. Єгоров С.В. Захист операційних систем від можливих загроз / Єгоров С.В. Вісник НАУ. 2011. №4.С. 80-82.

2. Домарєв В.В. Організація захисту інформації на об'єктах державної та підприємницької діяльності /Домарєв В.В., Скворцов С.О./ Навч. Посібник. — К.: Вид-во Європейського університету, 2006. — 102с.

УДК: 004.056.55: 003.26

А.В. Онацкий, к.т.н.

Одесская национальная академия связи им. А.С. Попова, onatsky@mail.ru

МОДИФИКАЦИЯ ПОРОГОВОЙ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА БЛЭКЛИ

Для защиты секретной информации от потери и компрометации необходимо повысить надежность хранения секретной информации. Одним из методов повышения надежности хранения секретной информации, является использование схем разделения секрета.

В криптографии под схемой разделением секрета понимают любой метод распределения секрета среди группы абонентов (участников), каждому из которых достается доля секрета. Схема разделения секрета состоит из двух основных фаз.

1. На фазе разделения секрета, дилер знающий секрет M, генерирует n долей секрета $b_1, b_2, \dots, b_n$ и посылает долю b_i абоненту A_i ($i = 1, \dots, n$) по каналу связи.

2. На фазе восстановления секрета M определенная группа абонентов m, собравшись вместе, и объединив свои доли секрета b_i однозначно восстанавливает секрет M. Причем любые (m — 1) и менее участников не могут этого сделать.

Наиболее известными пороговыми схемами разделения секрет являются: Миньотта, Асмута–Блума, Блэкли, Шамира, основанных на использовании мультипликативных полей. С развитием методов и средств криптоанализа, а также быстрого развития технологий и мощности вычислительных компьютерных систем, возникает необходимость увеличивать размеры общесистемных параметров схем разделения секрета, вследствие чего увеличивается ресурсоемкость и сложность выполнения базовых операций в полях. Однако решение данного вопроса может быть достигнуто за счет реализации схем разделения секрета на основе математического аппарата эллиптических кривых, что позволяет уменьшить размеры параметров схем и увеличить криптографическую стойкость.

В работе предложена модификация схемы разделения секрета Блэкли на эллиптических кривых. Параметрами схемы являются: n — число долей секрета; m — минимальный размер разрешенной группы; $E_p(a, b)$ — эллиптическая кривая (ЭК); $G = (x, y)$ — генерирующая точка ЭК; $\#E_p(a, b)$ — порядок группы кривой; M — секрет вложен в точку P_M ЭК.

Случайным образом дилер выбирает точки на эллиптической кривой P_2, $P_3, \dots, P_m$.

Фаза разделения секрета.

Для каждого абонента A_i дилер выбирает случайные равномерно распределенные на Z_p коэффициенты $a_{1i}, a_{2i}, a_{3i}, \dots, a_{mi}$ и вычисляет доли

$$b_i = a_{1i}P_M + a_{2i}P_2 + a_{3i}P_3 + \dots + a_{mi}P_m. \quad (1)$$

Абонентам раздаются числа $\{a_{1i}, a_{2i}, a_{3i}, \dots, a_{mi}, b_i\}$.

Фаза восстановления секрета:

Восстановить секрет M, имея b_i долей, можно решив систему уравнений

$$\begin{cases} a_{11}P_M + a_{21}P_2 + a_{31}P_3 + \ldots + a_{m1}P_m = b_1; \\ a_{12}P_M + a_{22}P_2 + a_{32}P_3 + \ldots + a_{m2}P_m = b_2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1m}P_M + a_{2m}P_2 + a_{3m}P_3 + \ldots + a_{mm}P_m = b_m. \end{cases} \qquad (2)$$

и получим секретную точку P_M.

Предложенная схема эллиптической пороговой схемы разделения секрета, основанная на использовании группового закона сложения элементов аддитивной абелевой группы на ЭК, существенно превосходит по криптографической стойкости аналогичных схем, основанных на использовании мультипликативных полей. Кроме того, сложность выполнения преобразования в абелевой группы на ЭК оценивается величиной $O(\log^2 p)$, а в мультипликативной группе поля — $O(\log^3 p)$, преимущество использования ЭК очевидно.

Разработанная схема разделения секрета на ЭК может быть использована в задачах передачи, хранения и обработки данных, требующих защиты от несанкционированного доступа.

УДК 621.391.54

О.І. Пікуль, С.В. Толюпа, проф.

Державний університет телекомунікацій

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ У МЕРЕЖАХ ЗВ'ЯЗКУ

Актуальність проблеми захисту інформації пов'язана з ростом можливостей обчислювальної техніки. Розвиток засобів, методів і форм автоматизації процесів обробки інформації і масове застосування персональних комп'ютерів роблять інформацію набагато більш уразливою.

В умовах широкого застосування обчислювальної техніки і засобів обміну інформацією поширюються можливості несанкціонованого використання або модифікації інформації. В зв'язку з чим захисту інформації від несанкціонованого доступу приділяється усе більше уваги. Особливо уразливі незахищені системи зв'язку, в тому числі обчислювальні мережі. Інформація, циркулююча в них, може бути незаконно змінена, викрадена або знищена. Останнім часом в засобах масової інформації з'явилася безліч сенсаційних повідомлень про факти злочинних впливів на апаратуру обробки, зберігання і передачі інформації, що нанесли великого матеріального збитку.

У літературі запропоновані різні визначення загроз в залежності від їх специфіки, середовища вияву, результату їх впливу. Під загрозами ми будемо розуміти цілеспрямовані дії, які підвищують уразливість інформації в інформаційній мережі, приводять до її випадкової або навмисної зміни або знищення.

Випадкові загрози включають в себе помилки, пропуски тощо, а також події, що не залежать від людини, наприклад природні явища (повінь,

землетрус) або викликаними діяльністю людини (пожежа, війна). Заходи захисту від них — в основному, організаційні.

До помилок апаратних і програмних засобів відносяться пошкодження комп'ютерів і периферійних пристроїв (магнітних носіїв тощо), помилки в прикладних програмах. До помилок через неувагу, досить часто виникаючих під час технологічного циклу обробки, передачі або зберігання даних, відносяться помилки користувача, оператора або програміста, втручання під час виконання програм, пошкодження носіїв інформації та інші. Навмисні загрози можуть реалізувати як внутрішні для системи учасники процесу обробки даних (персонал організації тощо), так і особи, так звані «хакери».

Навмисні загрози приводять до безпосереднього розкриття або зміни даних. Шкідливі програми інколи неправильно ототожнюють з комп'ютерними вірусами, тоді як віруси — лише одні з численних видів шкідливих програм.

Фізичні засоби захисту засновані на створенні фізичних перешкод для зловмисника, які перегороджують йому шлях до інформації (сувора система пропуску на територію і в приміщення з апаратурою або з носіями інформації). Ці засоби дають захист тільки від «зовнішніх» зловмисників і не захищають інформацію від тих осіб, які володіють правом входу в приміщення. До законодавчих засобів захисту відносяться законодавчі акти, які регламентують правила використання і обробки інформації обмеженого доступу і встановлюють заходи відповідальності за порушення цих правил.

Вибір засобів захисту інформації в інформаційних мережах — складна задача, при розв’язанні якої потрібно враховувати імовірності різних загроз інформації, вартість реалізації різних засобів захисту і наявність різних зацікавлених сторін. Користувачам важливо знати, що сучасна наука має в своєму розпорядженні методи, що дозволяють вибрати таку сукупність засобів захисту, яка забезпечить максимізацію заходів безпеки інформації при даних витратах або мінімізацію витрат при заданому рівні безпеки інформації.

УДК 336.221

В.Л. Плескач,
професор кафедри програмування та комп’ютерної техніки ФІТ КНУ ім.Тараса Шевченка, v_pleskach@ukr.net
М. В. Плескач
студентка 5 курсу КНУ ім.Тараса Шевченка, masha_plesk@ukr.net

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ РОЗБУДОВИ ДЕРЖАВНОСТІ

З розвитком інформаційного суспільства інформація є не тільки засобом забезпечення безпеки, а й може виступати як загроза та ризики. Саме цим зумовлена актуальність забезпечення інформаційної безпеки України як результат управління інформаційними загрозами з метою задоволення національних інтересів людини, суспільства та держави в інформаційній сфері.

Проблеми інформаційної безпеки України нині є надзвичайно актуальними. За умов глобальної інтеграції та міжнародної конкуренції головною сферою зіткнень і боротьби національних інтересів держав є інформаційний простір. Сучасні інформаційно-комунікаційні технології (ІКТ) надають змогу країнам реалізувати їх інтереси з їх допомогою, спричинити шкоду безпеці конкурентоспроможності іншої держави, яка не має дієвої системи захисту від негативних інформаційних впливів. За сучасних умов інформаційна безпека набуває все більшого значення і стає одним із найважливіших елементів забезпечення національної безпеки, державного, інформаційного суверенітету.

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації[1]. Серед першочергових пріоритетів Стратегії 2020[2] за вектором безпеки є: реформа системи національної безпеки та оборони; реформа оборонно-промислового комплексу; судова реформа; оновлення влади та антикорупційна реформа; програма електронного урядування; реформа правоохоронної системи; програма енергонезалежності; реформа захисту інтелектуальної власності і програма збереження навколишнього природного середовища.

За умови забезпечення належного рівня інформаційної безпеки держави можливим є стійкий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у різних сферах, захист конституційних прав і свобод людини і громадянина, духовних, культурних засад суспільства, конституційного ладу, суверенітету, у тому числі інформаційного, територіальної цілісності і недоторканності держави, гарантування права кожного одержувати, використовувати, зберігати інформацію з будь-якого джерела, не забороненого законодавством, забезпечення пріоритетного розвитку національних інформаційних ресурсів; забезпечення сприяння побудові в Україні розвинутого інформаційного суспільства. Попри важливість зазначеної проблематики, вона не є дослідженою в повному обсязі. На сьогодні нерозв'язаними залишаються такі проблеми, зокрема необхідним є:

– розроблення і розвиток, обґрунтування понятійно-категоріального апарату у сфері інформаційної безпеки;

– вдосконалення нормативно-правового регулювання інформаційної безпеки України. На сьогодні не прийнято закону, який би визначав Концепцію державної інформаційної політики України. До того ж, у квітні 2014 року Указом Президента було визнано такою, що втратила чинність Доктрина інформаційної безпеки України від 2009 р., що є гострим викликом в нинішніх складних, кризових умовах. У цьому контексті, доцільно щомога пришвидшити

[1] Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 р.р.: [закон України: офіц. текст: за станом на 9 січня 2007р.] // Відомості Верховної Ради України (ВВР). — 2007. — № 12.
[2] http://zakon4.rada.gov.ua/laws/show/5/2015.

розроблення нової Доктрини інформаційної безпеки, яка б відповідала вимогам часу;

– захист національного інформаційного простору України від розповсюдження викривленої або забороненої для поширення законодавством України інформаційної продукції;

– встановлення законодавством правил доступу інших держав або їхніх представників до державних інформаційних ресурсів України та порядку їх використання;

– законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва в Україні;

– удосконалення системи управління інформаційною безпекою як на державному, так і на місцевому рівнях;

– створення і використання інформаційно-аналітичного забезпечення для прийняття управлінських рішень органами державної влади, громадянами, іншими суб'єктами права в Україні;

– гарантування свободи інформаційної діяльності та права доступу до інформації в національному інформаційному просторі України; всебічний розвиток національної інформаційної інфраструктури, законодавче окреслення допустимих меж інформаційного моніторингу за умов військових дій та проведення антитерористичної операції;

– підтримка державою розвитку національних інформаційних ресурсів з урахуванням новітніх технологій;

– розроблення та впровадження безпечних ІКТ;

– створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом тощо.

Висновки. Отже, із вищезазначеного випливає, що інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, захисту державного суверенітету. Потребує особливої уваги система забезпечення інформаційної безпеки України, зокрема відповідне реалістичне матеріально-технічне та державне фінансове забезпечення їх функціонування. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

УДК 004.056.5

Поліщук К.А

Державний університет телекомунікацій

ПРОЦЕСНИЙ ПІДХІД В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

У результаті інтенсивного використання інформаційних технологій практично в усіх сферах діяльності задачі управління сучасною організацією та її Інформаційною безпекою з кожним днем стають все складнішими.

Згідно ISO 27001, система управління інформаційною безпекою (СУІБ) — це «та частина загальної системи управління організації, заснованої на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки». Система управління включає в себе організаційну структуру, політики, планування, посадові обов'язки, практики, процедури, процеси і ресурси.

У разі прийняття рішення про створення СУІБ слід чітко розуміти, що це не разовий захід, а постійна робота, оскільки ефективність процедур системи управління може з плином часу знижуватися.

Всі процедури процесного підходу до управління повинні послідовно проходити наступні чотири етапи: Кожен етап характеризується виконанням різних процедур.

Етапи функціонування можна описати так:

1. Планування процедур СУІБ:

2. Впровадження процедур СУІБ:

3. Моніторинг та аналіз процедур СУІБ:

4. Удосконалення СУІБ:

Кожен етап характеризується виконанням різних процедур.

Розглянувши основні етапи створення СУІБ,можна сказати , що цей підхід закладений в міжнародних стандартах на системи управління, в тому числі і ISO / IEC 27001 досить складний і тривалий. Зусилля, витрачені на створення системи управління інформаційною безпекою, дозволять організації вийти на новий вищий рівень.

ЛІТЕРАТУРА:

1. В.А. Трайнёв, А.А. Федулов «Информационная безопасность» ИТК Дашков и К, 2005. — 336 с.

2. Система управления информационной безопасностью в соответствии с ISO/IEC

УДК 004.056.5

В.В. Приступа, к.т.н.

ПАТ «Державний ощадний банк України», PrystupaVV@oschadbank.ua

КОНЦЕПТУАЛЬНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БАНКІВСЬКІЙ СИСТЕМІ

Виходячи з вимог чинного законодавства України та загального стану у питаннях захисту електронної інформації в Банківській системі одним з першочергових завдань є створення ефективної системи управління інформаційною безпекою (СУІБ). Підґрунтям цих вимог є Постанова Правління НБУ від 28.10.2010 р. № 474, яка вимагає від банків України впровадження СУІБ відповідно до галузевих стандартів Національного банку України — СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010 (надалі — Галузеві стандарти).

Побудова системи управління інформаційною безпекою передбачає створення ефективної управлінської моделі, що забезпечує функціонування СУІБ (функціонування Комітету СУІБ, визначення власників інформаційних активів, опис бізнес-процесів та аналіз ризиків інформаційної безпеки, впровадження відповідних нормативних документів тощо). При цьому для впровадження ряду контролів СУІБ (наприклад моніторинг дій користувачів та адміністраторів, своєчасне реагування на інциденти тощо) є необхідність застосування технічних засобів захисту інформації. З метою забезпечення централізованого управління процесами/ процедурами інформаційної безпеки та якісного та оперативного реагування на інциденти за єдиними правилами на даний час існує необхідність інтеграції всіх технічних засобів до єдиної системи захисту інформації.

Застосування цих засобів захисту продиктоване також наявністю інших вимог щодо захисту електронної інформації з обмеженим доступом (банківська таємниця, персональні данні, комерційна таємниця тощо), що наявні у чинному законодавстві України, нормативних документах НБУ та внутрішніх нормативних документах Банків. Здебільшого ці вимоги визначаються на підставі реалій сьогодення у сфері розвитку інформаційних технологій та загроз на які наражаються процеси обробки інформації.

Сучасні технічні засоби захисту інформації сегментовані виробниками за напрямками забезпечення контролів інформаційної безпеки. Розробка та виробництво цих засобів орієнтовані на виконання, у першу чергу, вимог міжнародних стандартів з інформаційної безпеки, таких як стандарти серії ISO 27XXX, модифікацією яких є Галузеві стандарти.

Враховуючи це, а також аналіз контролів, наявність яких вимагається Галузевими стандартами, та технічних засобів за напрямками забезпечення інформаційної безпеки Орієнтовний перелік технічних засобів захисту інформації, що дають змогу забезпечити виконання вимог стандартів СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010 складає:

- Підсистема контролю цілісності;
- Підсистема антивірусного захисту;
- Підсистема захищеного зберігання інформації;
- Підсистема контролю відповідності вимогам політик і стандартів;
- Підсистема сканування вразливостей;
- Підсистема попередження витоку інформації;
- Підсистема виявлення та запобігання вторгненням;
- Підсистема контролю дій адміністраторів;
- Підсистема доступу до інформаційних ресурсів з використанням двохфакторної автентифікації;
- Підсистема управління інцидентами інформаційної безпеки.

УДК 004.056.54

Д.А. Прогонов, Д.О. Паничева, А.В. Дорошенко
Физико-технический институт, НТУ Украины
«Киевский политехнический институт»
progonov@gmail.com

ИСПОЛЬЗОВАНИЕ ПАКЕТА ТЕСТОВ NIST ДЛЯ ОПРЕДЕЛЕНИЯ ОБЛАСТИ ВСТРАИВАНИЯ СТЕГОДАННЫХ В КОНТЕЙНЕР

Для повышения эффективности активного стегоанализа в случае, когда в качестве контейнеров используются цифровые изображения (ЦИ), необходима априорная информация о методе, примененном для встраивания стегоданных в контейнер, а также области скрытия сообщений. Существующие методы стегоанализа ЦИ (например, статистический анализ [1-3]) позволяют определить лишь факт наличия стеганограм, поэтому представляет интерес исследование специальных методов анализа ЦИ для определения области скрытия сообщений.

В работе рассмотрено использование пакета тестов NIST для оценки искажений статистических характеристик шумов цифровых изображений (ЦИ) при встраивании стегоданных в различные области контейнера — в пространственную область (Least Significant Bits (LSB) методы) и в области преобразования контейнера. Исследование проводилось с использованием метода Куттера-Джордана-Боссена (МКДБ), относящегося к классу LSB-методов, а также метода Кима, в соответствии с которым, сообщения встраивались в частотной области ЦИ [4]. Степень заполнения контейнера стегоданными варьировалась от 5% до 25%, с шагом 5%, и от 25% до 95% с шагом 10%.

Установлено, что скрытие данных в пространственной и частотной областях контейнера приводит к появлению характерных изменений статистических характеристик шумов ЦИ. Сравнение, проведенное для МКДБ и метода Кима, показало резкие отличия в результатах прохождения тестов NIST. При скрытии сообщений в ЦИ согласно МКДБ наибольшие отклонения от среднестатистических параметров были выявлены при исследовании стеганограмм с применением теста на линейную сложность, а при использовании метода Кима — при прохождении теста рангов бинарных матриц и теста на линейную сложность, что может быть использовано для определения области скрытия данных в контейнере.

Полученные данные могут быть полезными при разработке новых, эффективных методов пассивного стегоанализа цифровых изображений, позволяющих определять область встраивания стегоданных.

Список литературы:

1. Fridrich J. Rich models for steganalysis of digital images / J. Fridrich, J. Kodovsky // IEEE Transactions on Information Forensics and Security. — 2012. — Vol. 7, Issue 3. — p. 868-882.

2. Kodovsky J. Steganalysis of JPEG Images Using Rich Models / J. Kodovsky, J. Fridrich // Electronic Imaging, Media Watermarking, Security, and

Forensics. Proceedings of 14th SPIE conference. — San Francisco, California, USA. January 23–25, 2012. — Vol. 8303. — p. 1-12.

3. Holub V. Random Projections of Residuals as an Alternative to Co-occurrences in Steganalysis / V. Holub, J. Fridrich, T. Denemark / Electronic Imaging, Media Watermarking, Security, and Forensics. Proceedings of 15th SPIE conference. — San Francisco, California, USA. March 22, 2013. — Vol. 8665. — DOI:10.1117/12.1000330.

4. Chol-Su Kim. Document watermarking based on digital holographic principle / Chol-Su Kim, Kwang-Hyok Jong, Song-Jin Im // Institute of Optics, Department of Physics, Kim Il Sung University, Pyongyang, DPR of Korea — 2013

УДК 004.(056:932.4)

Д.А. Прогонов, К.В. Черепахова, М.А. Чипак

Физико-технический институт, НТУ Украины

«Киевский политехнический институт», progonov@gmail.com

ОБНАРУЖЕНИЕ И ПОДАВЛЕНИЕ СООБЩЕНИЙ, ВСТРОЕННЫХ В КОНТЕЙНЕРЫ НА ОСНОВЕ LSB-МЕТОДОВ

В настоящее время для скрытия сообщений в цифровых изображениях (ЦИ) широко используются Least Significant Bits (LSB) методы [1]. Данные методы характеризуются сравнительно невысокими требованиями к параметрам контейнера и позволяют проводить встраивание стегоданных в режиме реального времени.

Для обнаружения стеганограмм, сформированных на основе LSB-методов, широко применяются стандартные статистические методы [2, 3]. Существенным ограничением таких методов является низкая вероятность обнаружения стеганограмм при слабом заполнении контейнера стегоданными.

Искажения сообщений, встроенных в изображения, обеспечиваются применением стандартных методов обработки ЦИ (например, сжатия, фильтрации). Однако в этих случаях, применяя специальные методы при проведении экстракции стегоданных, возможно скомпенсировать искажения встроенных сообщений. Поэтому актуальной является задача поиска новых методов стегоанализа ЦИ для обнаружения стеганограмм и внесения необратимых искажений в стегоданные.

В работе рассмотрена возможность использования Rescaled Range (R/S) анализа при проверке ЦИ на наличие стегоданных. Получены параметры распределения значений показателя Херста (ПХ), математическое ожидание, дисперсия и другие, в зависимости от степени заполнения контейнера стегоданными (от 5% до 95%). Показано, что применение LSB-методов при формировании стеганограмм приводит к существенному изменению параметров распределения значений ПХ (например, коэффициентов асимметрии и эксцесса) по сравнению с аналогичными параметрами незаполненного контейнера.

Проведен сравнительный анализ эффективности деструкции стегоданных с использованием различных методов обработки ЦИ (γ^{-}коррекции, метода

CLAHE (Contrast Limited Adaptive Histogram Equalization), медианной фильтрации (МФ) и двумерной винеровской фильтрации (ДВФ)). Оценка эффективности методов обработки проводилась по мощности ансамбля неизмененных бит стегоданных. Отмечено, что при использовании МФ достигается максимальная степень искажения стегоданных, но возникают существенные визуальные искажения ЦИ. ДВФ обеспечивает высокий уровень искажения встроенных сообщений при меньших искажениях стеганограмм по сравнению с МФ. Применение $\gamma-$коррекции и метода CLAHE позволяет минимизировать визуальные искажения ЦИ, но при этом степень искажения стегоданных меньше, чем у МФ и ДВФ.

Полученные результаты могут быть использованы для повышения точности обнаружения стеганограмм при малых степенях заполнения контейнера стегоданными и оптимизации существующих методов деструкции встроенных сообщений.

Список литературы:

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Конахович Г.Ф., Пузыренко А.Ю. — К.: «МК-Пресс», 2006. — 288 с., ил.

2. T. Pevny Steganalysis by Subtractive Pixel Adjacency Matrix / T. Pevny, P. Bas, J. Fridrich // IEEE Trans. on Info. Forensics and Security. — 2010. — Vol. 5, Issue 2. — p. 215-224.

3. Прогонов Д., Кущ С. Оценка эффективности статистических методов стегоанализа 2D-контейнеров. — Сборник тезисов XVI Международной научно-практической конференции «Безопасность информации в информационно-телекоммуникационных системах». — К.: ООО «ИП Эдельвейс», 2013. — с. 52.

УДК 004.056.5

Р.Б. Прус, к.т.н.

Київський національний університет імені Тараса Шевченка,
ruslana_prus@meta.ua

АНАЛІЗ УРАЗЛИВОСТЕЙ ОБ’ЄКТІВ ЗАХИСТУ ІНФОРМАЦІЇ

В умовах активного розвитку інформаційних систем та нових технологій несанкціонованого доступу до інформації зростають вимоги до ефективності систем захисту інформації.

З метою оцінки та прогнозування стану інформаційної безпеки запропоновано модель прогнозування наслідків почергового прийняття рішень сторонами нападу і захисту у динамічному режимі [1]. У результаті отримано оптимальний набір рішень нападу і захисту, які в теорії ігор складають рівновагу за Нешем. Модель дає змогу оцінити рівень очікуваних втрат та обрати рішення, що гарантує мінімальну очікувану шкоду від реалізації загроз при найбільш несприятливих умовах.

При моделюванні використано функцію уразливості об’єктів, що залежить від розміру інвестицій обох сторін та може описувати різні системи. Функції уразливості включають параметри, що дають змогу визначити зони

найбільшої економічної доцільності витрат в складних системах захисту інформації, що дозволяє підвищити ефективність використання внесених інвестицій [2].

У результаті аналізу уразливостей виявляються, ідентифікуються та класифікуються уразливості комп'ютерів, серверів, мережі та мережевого обладнання, а також програмного забезпечення. Аналіз уразливостей дає можливість прогнозувати ефективність контрзаходів та оцінити їхню роботу. Створюється база даних, що містить усю необхідну інформацію для перевірки системи на наявність прогалин у системі безпеки, аномалій у мережі, потенційних шляхів проникнення у систему через недоліки програмного забезпечення.

Система аналізу уразливостей ефективна, якщо виконуються умови:

- інформація про нові уразливості постійно оновлюється;
- при виявленні уразливостей число хибнопозитивних результатів не перевищує допустимого значення;
- здатність проводити перевірку кількох систем одночасно;
- за результатами перевірок складаються чіткі та зрозумілі звіти;
- надаються рекомендації щодо контрзаходів для усунення виявлених уразливостей.

Аналіз уразливостей складається із таких етапів:

- визначаються та класифікуються об'єкти мережі або системи;
- оцінюється важливість кожного об'єкта;
- визначаються потенційні загрози, джерела їх виникнення (на цьому етапі система піддається умисним атакам з метою виявлення уразливостей);
- розробляється план своєчасної протидії найнебезпечнішим загрозам у першу чергу;
- здійснюються заходи щодо мінімізації завданої шкоди у разі реалізації загроз.

З метою проведення результативного аналізу уразливостей проводиться моніторинг безпеки, увага зосереджуєтсья на найбільш критичних об'єктах і посилюються превентивні заходи для запобігання виникнення загроз; проводиться розслідування інцидентів інформаційної безпеки.

Список використаних джерел:

1. Прус Р.Б. Оптимізація розподілу ресурсів захисту інформації в динамічному режимі / Р.Б. Прус // Безпека інформації. — 2012. — №1. — С. 26-32.

2. Левченко Є.Г. Оптимізаційні задачі менеджменту інформаційної безпеки / Є.Г.Левченко, А.О. Рабчун // Сучасний захист інформації. — 2010. — №1. — С.16-23.

УДК 004.7

І.В. Рубан, д.т.н. професор, Є.С. Лошаков
Харківський університет Повітряних Сил імені І.М. Кожедуба, stforge@mail.ru

СИСТЕМА ПРОТИДІЇ ПОВІЛЬНИМ DOS-АТАКАМ

В кінці XX століття все більшого розвитку набувають інформаційні технології. Вони проникають в усі сфери людської діяльності. З одного боку, це призводить до значного підвищення ефективності праці в наслідок впровадження систем автоматизації та засобів обробки і передачі інформації. А з іншого — стає причиною виникнення такого виду злочинності, як інформаційна. Паралельно з розвитком інформаційних технологій розвиваються різноманітні засоби несанкціонованого доступу до інформації та порушення працездатності інформаційно-телекомунікаційних систем. Вони становлять істотну загрозу інформаційній безпеці інформаційно-телекомунікаційних систем як великих корпорацій, так і державних установ, про що свідчить значна кількість успішно проведених кібернетичних атак по всьому світі. Існує велика кількість загроз інформаційній безпеці. Постійно з'являються нові види кібернетичних атак. Одними з найбільш розповсюджених видів атак є атаки типу «відмова в обслуговуванні» (DoS-атаки). На теперішній час відома значна кількість способів реалізації даної атаки. Існують засоби виявлення та протидії усім відомим реалізаціям DoS-атаки, крім повільної DoS-атаки, що реалізується завдяки особливостям функціонування протоколу TCP.

Для виявлення та подальшого блокування повільних DoS-атак запропоновано систему протидії, яка представляє собою програмно-апаратний комплекс, що впроваджується в інформаційно-телекомунікаційну систему. В ньому реалізується механізм аналізу вхідного трафіку, механізм виявлення джерел шкідливого трафіку та механізм блокування цих джерел.

Вхідний трафік аналізується на предмет наявності характерних для повільної DoS-атаки піків трафіку, що мають місце у каналі зв'язку в певні моменти часу, обумовлені особливостями роботи протоколу TCP, а також контролюється надходження від адресатів підтверджень про отримання відправлених пакетів. При цьому усі вхідні сегменти записуються в базу даних. Якщо повільна DoS-атака має місце, запускається механізм виявлення джерел шкідливого трафіку.

Цей механізм реалізується наступним чином. З бази даних виділяються сегменти, що були отримані в інтервали часу, в які очікується надходження шкідливого трафіку, проводиться сортування сегментів за їх вихідним програмним портом та визначається порт, з якого прибуло найбільше сегментів. Після цього трафік, що надходить з цього порта блокується.

Механізм блокування реалізується шляхом підміни вихідної IP-адреси сервера, що атакується, на IP-адресу програмного маршрутизатора, що є резервним у даній інформаційно-телекомунікаційній мережі. Внаслідок чого, подальший шкідливий трафік надходить на програмний маршрутизатор, а сервер продовжує надавати послуги своїм легітимним користувачам.

Список використаних джерел:

1. Юрий Жуков. Основы веб-хакинга. Нападение и защита. — СПб.: Питер, 2006. — 208 с.

2. Рубан І.В. Обґрунтування вибору інтервалу спостереження при очікуванні повільної DoS-атаки / І. В. Рубан, Є.С. Лошаков, Д.В. Прибильнов // Системи обробки інформації. — 2014. — Вип. 8. — С. 135-137.

УДК 003.26.09 : 004.056.55

Д. М. Самойленко

Національний університет кораблебудування ім. адмірала Макарова / Збройні Сили України, DenNikSam@gmail.com

ДИНАМІЧНИЙ СТЕГОЗАХИСТ МЕРЕЖНОГО РЕСУРСУ

Останнім часом для покращення захисту мережних інформаційних ресурсів була розвинена методика динамічної стеганографії, тобто прихованої інтервенції захисних ознак з постійним оновленням. Зазначена методика надає змогу відрізняти поточний елемент від застарілого (узятого з попередньо завантаженого МІР) чи підробленого. Методика була успішно випробувана для текстових та графічних об’єктів МІР.

Пропонується адаптування динамічного стегозахисту для виконавчого коду МІР (клієнтської частини). Головною ідеєю є використання різних програмних реалізацій для тіла однієї і тієї ж функції при різних сеансах клієнт-серверної взаємодії, тобто впровадження псевдо поліморфного коду.

Подібно до методу знаків однакового нарису, розвиненому для текстової стеганографії, для програмного коду можна запропонувати метод елементів однакової семантики. Закладений у суть вихідного методу факт того, що заміна знаків англійської абетки на знаки української не змінює сприйняття тексту «на око», проте дозволяє виявити їх програмно, цілком аналогічний твердженню, що заміна програмних елементів однакової семантики (імен змінних, функцій, об’єктів та їх методів чи властивостей, тощо, а також порядку їх оголошення) на інші не змінить функціональність коду, проте дозволить відрізнити один код від іншого. Слід лише зауважити, що зазначена заміна має бути синхронною у всьому коді в межах області видимості відповідних елементів. Асинхронно можливо здійснювати заміну роздільних символів, на зразок «пробіл» — «табуляція».

а методом елементів однакової семантики можна описати у вигляді алгоритму та проілюструвати на прикладі у наступний спосіб:

1. Сервер формує певний шаблон для тіла функції, використовуючи спеціальні текстові конструкції, що у подальшому будуть замінені на однакові елементи коду.

$placeholder='function_WM1_fun(){…}';

У наведеному коді у шаблоні ($placeholder) передбачається підстановка замість конструкцій _WM1_ довільного роздільного знаку.

2. Для конкретного сеансу клієнт-серверної комунікації обирається зміст кожного з елементів для заміни та формується виконавчий код:

```
$code=str_replace("_WM1_","\t",$placeholder);
```

У прикладі використано функцію заміни рядків (str_replace), замість конструкцій _WM1_ виконано підстановку символу табуляції, результат заміни збережено у змінній ($code).

3. Обчислюється хеш-образ сформованого коду і зберігається для кожного клієнта, що звертається до сервера

```
$hash=sha1($code);
```

Для демонстрування використано стандартну хеш-функцію мови PHP (sha1), очевидно, що можливо впровадження довільного криптографічного перетворення.

4. Сформований код передається до клієнта у складі активних скриптів

```
echo "<script> $code </script>";
```

За наявності спеціального запиту від сервера на самотестування або безумовно, у кожному з запитів активні скрипти додають до даних, що передаються серверу, контрольні хеш образи.

5. Отримавши відповідь від клієнта сервер аналізує передане та збережене значення образу та приймає рішення щодо результатів контролю цілісності.

Випробування алгоритму засвідчило його дієвість щодо можливості розрізнення завантаженої версії сторінки. Останнє дозволяє покращити інформаційну безпеку МІР у контексті контролю засобів формування програмних запитів.

УДК 621.386.4

Скрипник В.В., Жураковський Б.Ю.

Державний університет телекомунікацій

ІНТЕЛЕКТУАЛЬНИЙ ПІДХІД ДО УПРАВЛІННЯ МЕРЕЖНИМИ ВІДМОВАМИ СИСТЕМ ПЕРЕДАЧІ ДАНИХ

Актуальність проблеми. В даний час немає жодної області людської діяльності, яка не використала б можливості сучасних інформаційних та інтелектуальних технологій в галузі телекомунікацій. Сьогодні ми є свідками стрімкого розвитку мереж нового покоління *NGN*, мультисервісних мереж передачі даних (СПД), що виконують обробку й передачу всіх типів даних і інформації, доступ до яких можна отримати в будь-якій точці світу.

Мережі передачі даних, будучи складною організаційно-технічною системою, повинна забезпечити безперебійне і повноцінне функціонування всіх компонентів і гарантувати надання користувачам послуг зв’язку і інформатизації, відповідно до прийнятих оператором зв’язку на себе зобов’язаннями.

Із зростанням розмірів, складності устаткування і функціональних можливостей в значній мірі збільшується відповідальність посадовців за правильність і обґрунтованість рішень, які ухвалюються, для ефективного управління СПД. Крім того, посадовцям доводиться ухвалювати рішення в умовах неповної інформації про стан елементів мережі, обмеженого часу на аналіз проблемних ситуацій. Все це приводить до невідповідності можливостей людини та складності завдань, які необхідно вирішувати для підтримки мережі в працездатному стані, зокрема за рахунок використання сучасних методів її діагностики. У зв'язку з цим **розробка і впровадження інтелектуальних технологій для діагностики сучасних систем телекомунікацій є актуальним науково-технічним завданням.**

Проведений аналіз сучасних систем управління телекомунікаційними мережами, зокрема завдань моніторингу, аналізу і діагностики мережевих процесів показав, що ці завдання входять в критичну безліч завдань по управлінню мережевими ресурсами і для їх вирішення потрібна активна участь фахівця і використання різних (у тому числі і комп'ютерних) систем забезпечення його діяльності. Аналіз методів діагностики мережевих відмов (МВ) (сигнатурний, статистичний аналіз, використання інтелектуальних (експертних) систем, генетичних алгоритмів, нейромереж і т. ін.), і на підставі порівняльного аналізу моделей діагностики МВ зроблений висновок про доцільність застосування комплексного підходу до рішення задач діагностики СПД, що включає статистичні методи, в доповненні до сигнатурних систем, що застосовуються на практиці, а як система, що дає можливість прийняти правильне рішення, використовувати інтелектуальну (експертну) систему. Практика показує, що у посадовців, від яких залежить якість і надійність функционірованія СПД, украй мало часу на аналітичну роботу, що дозволяє уникнути помилок при ухваленні рішень. Кращим варіантом організації підтримки діяльності осіб, що ухвалюють рішення, є створення навколо них середовища людино-машинної підтримки, в якій головна роль відводилася б системи підтримки прийняття рішень.

ЛІТЕРАТУРА

1. Борисов А.Н., Алексеев А.В., Меркур'єва Г.В. и др. Обработка нечеткой информации в системах принятия решений. — Г.: Радио и связь, 1989. — 304 с.
2. Герасимов Б.М., Тарасов В.А., Токарев И.В. Человеко-машинные системы принятия решений с элементами искусственного интеллекта. — К.: Нукова мысль, 1993. — 184 с.
3. Нечеткие великого множества в моделях управления и искуственного интеллекта. Под ред. Д.А. Поспєлова. -Г.:Наука, 1986.—311с.

УДК 621.376.54

М.І. Стойчев, В.П. Новіков, проф.
Державнй університет телекомунікацій

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НА ОСНОВІ МЕТОДУ ЕНЕРГЕТИЧНО-ЕФЕКТИВНОГО ПЕРЕТВОРЕННЯ ІКМ-СИГНАЛІВ

Одним з головних завдань, які вирішуються при створенні та функціонуванні інфокомунікаційних систем спеціального призначення (ІКС СП) є забезпечення належного рівня безпеки інформації. Вирішення цього завдання покладається на систему захисту інформації (СЗІ), як невід'ємну складову ІКС.

Аналіз загроз безпеці інформації та методів захисту від них, проведений в [1] показав, що поряд з криптографічними методами захисту інформації одним з основних напрямків забезпечення безпеки інформації в інфокомунікаційних систем спеціального призначення є застосування методів підвищення прихованості передачі сигналів. Тому вдосконалення існуючих та розробка нових методів формування та обробки сигналів, спрямованих на підвищення прихованості та енергетичної ефективності є перспективним напрямком досліджень у галузі інформаційної безпеки.

В статті запропоновано рішення другого аспекту задачі, шляхом формування принципово нової, порівняно з ІКМ, структури цифрового сигналу. При перетворенні початкового сигналу (стандартного сигналу ІКМ) такі характеристики системи, як необхідна смуга частот, завадостійкість та інформаційна швидкість передачі, потрібно зберегти незмінними, такими ж, як і у відповідних структур ІКМ сигналів. Це дасть можливість застосовувати даний спосіб на діючих телекомунікаційних трасах стандарту Е1.

Сутність розробленого методу полягає в тому, що замість кожної *k*-розрядної кодової комбінації окремого канального інтервалу (КІ) формується лише один імпульс-символ, в якому цифрова інформація, на відміну від ІКМ, міститься не в розміщенні нульових і одиничних імпульсів на відповідних розрядних позиціях кодової комбінації, а в номері тієї квантованої часової позиції, на якій розміщується цей одиночний імпульс [5, 6]. Назвемо такий інформаційно-насичений імпульс, що містить інформацію про всю кодову комбінацію, позиційним код-імпульсом (ПКІ).

Для оцінки ефективності [9] розробленого методу було створено імітаційну модель в середовищі програмування *MatLab*. Результати моделювання показали, що при використанні ПВП, які повністю ортогональні між собою, енергетична ефективність системи передачі інформації підвищується в 2,2 рази, порівняно зі стандартною ІКМ-системою. При використанні реальних ПВП (які не є повністю ортогональними) енергетичний виграш складає близько 15-20%.

Висновки. Таким чином, використання розробленого методу підвищує енергетичну ефективність при передачі сигналів в інформаційно-телекомунікаційних системах спеціального призначення, що в свою чергу дозволяє покращити прихованість та завадозахищеність, а значить, й інформаційну безпеку взагалі. Перевагою отриманої внаслідок запропонованих перетворень структури сигналу є, також, набуття властивостей шумоподібності, що, в свою чергу, підвищує прихованість передачі інформації. Така малопотужна шумоподібна суміш групового сигналу може передаватися, не створюючи завад сусіднім радіоелектронним засобам, які працюють в тому ж діапазоні частот. При цьому, також, ускладнюється розкриття факту передачі засобами радіотехнічної розвідки.

УДК 004.931

В.А.Темников, И.В.Конфорович
Национальный авиационный университет
temnikov_v@ukr.net

СИСТЕМА ВНУТРИСМЕННОЙ ГОЛОСОВОЙ АУТЕНТИФИКАЦИИ АВИАДИСПЕТЧЕРОВ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Безопасность полетов в авиации существенно зависит от правильности действий диспетчеров управления воздушным движением (авиадиспетчеров). Ошибки в их работе могут быть связаны с постоянным нервно-эмоциональным напряжением, вызванным повышенной ответственностью за принимаемые решения и дефицитом времени, а также несанкционированными действиями персонала.

Между тем, в настоящее время за действиями авиадиспетчеров во время выполнения ими своих функциональных обязанностей осуществляется лишь визуальный контроль. Поэтому одним из путей снижения количества аварий и аварийных ситуаций, имеющих место вследствие наличия человеческого фактора, является совершенствование контроля за действиями авиадиспетчеров во время рабочей смены (внутрисменного контроля их доступа к информационным ресурсам), заключающегося в проведении перманентных аутентификации и мониторинга психофизиологического состояния (эмоционального состояния, состояний утомления, сонливости, тревоги).

В докладе представлены принципы построения и результаты практической реализации основных подсистем разработанной авторами системы голосовой аутентификации, обеспечивающей дистанционный автоматический контроль авиадиспетчеров в режиме реального времени. Аутентификация осуществляется по непрерывной слитной речи авиадиспетчера на основе анализа параметров речевого сигнала, сканируемого в процессе аудиообмена авиадиспетчеров и членов летных экипажей.

Аутентификация проводится с применением методов теории распознавания образов на основе параметризации ключевых речевых

фрагментов, выделяемых из непрерывной слитной речи авиадиспетчеров. В качестве указанных речевых фрагментов используются отдельные слова и словосочетания, входящие в состав нормативно установленной профессиональной фразеологии авиадиспетчеров.

На основе проведенных исследований авторами разработана система информативных параметров речевых сигналов, в основе которой лежат амплитуды спектральных составляющих, полученных в результате быстрого преобразования Фурье «нового» сигнала, составленного из кепстральных коэффициентов линейного предсказания. Разработан алгоритм расчета предложенных информативных параметров речевого сигнала.

Вследствие достигнутого существенного (на порядок) уменьшения количества информативных параметров, требуемого для работы системы аутентификации, появилась возможность построить подсистемы классификации авиадиспетчеров и выделения ключевых речевых фрагментов из их непрерывной речи на основе искусственных нейронных сетей (ИНС). Конкретные вид ИНС и значения параметров подсистем параметризации и классификации были определены в процессе совместного тестирования этих подсистем по критерию максимума процента правильной аутентификации с учетом необходимого времени обучения ИНС и скорости обработки речевых сигналов.

Реализация представленных в докладе путей повышения быстродействия и точности работы систем аутентификации авиадиспетчеров позволила создать систему дистанционного автоматического голосового контроля доступа авиадиспетчеров к информационным ресурсам, обладающую более высокими быстродействием и точностью работы по сравнению с существующими системами. Процент правильной аутентификации в процессе экспериментальных исследований характеристик разработанной системы превышал 98%, а достигнутое быстродействие системы (время параметризации составляло порядка 10…25 мс) позволяет проводить аутентификацию в режиме реального времени.

UDC 681.5.004.94

O. M. Terentiev, PhD.
Institute for applied system analysis NTUU "KPI", Kyiv, Ukraine, o.terentiev@gmail.com
T. I. Prosyankina-Zharova
European University, t.pruman@gmail.com

MODELING OF INFORMATION DISSEMINATION USING THE CELLULAR AUTOMATA

It is difficult to overestimate the role of the impact of information society in the modern world. Within the conception of complex systems was developed natural computation, which involves mathematical methods based on the native mechanisms for decision-making.

As part of the research project NUKR.SFPP G4877 "Modeling and Mitigation of Social Disasters Caused by Catastrophes and Terrorism" (NATO scientific program "Science for Peace and Security") were investigated the rate of information dissemination throughout changing the number and density of information sources.

To conduct a series of computational experiments were set up the following rules.

1. Each cell has its own preset threshold value of information perception.

2. The size of the space 100 to 100 cells. The maximum number of cycles simulation 100. The number of information sources changes from 1 to 10.

3. Simulated space contains several anomalous areas (1) with increased level of information perception and (2) with a reduced level. In real life, these areas could be interpreted as a low and high sensitivity towards hostile information influence.

4. Each cell could take one of three states: (1) neutral, (2) receiving new information, (3) remembering information. A Bayesian approach was used to make a decision on the adoption of information cell [1].

As a simulation environment was used cloud services SAS Studio ODA (Online On Demand for Academics). SAS IML (Interactive Matrix Language) and SAS Base were used for programming mathematical algorithms.

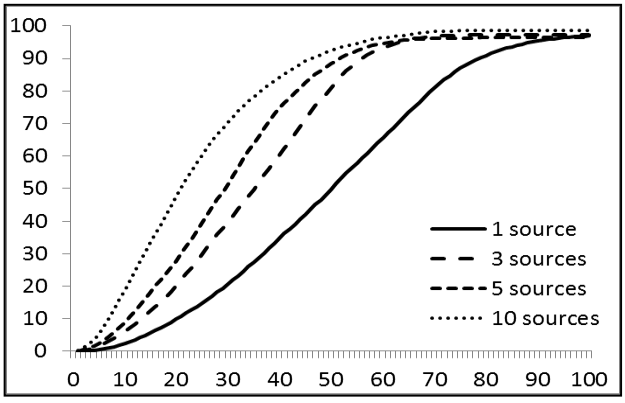


Figure 1. Results of modeling. OX is number of iteration and OY is the percentage of cells which were exposed

Figure 1 shows the simulation results. As a quantitative metric for comparing the scenarios proposed to use the value of the area under the curve of the integrand. The results showed that the speed of information propagation depends not only on the number of information sources, but also the degree of density location. In real life, this fact is expressed in the form of proper identification of appropriate communication canal towards to the defined target groups.

List of literature

1. Braichevskii, S.M. Lande, D.V. Urgent aspects of current information flow // Scientific and technical information processing. — Allerton press, inc. — Vol 32, part 6. -2005. — P. 18-31

УДК 621.266.21

С.В. Толюпа, І.М. Павлов

Державний університет телекомунікацій

МОДЕЛЮВАННЯ ПРОЦЕСІВ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ПРОЕКТУВАННІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Постановка проблеми. У багатьох ситуаціях проектування систем захисту інформації виникає необхідність розробки та прийняття рішень в умовах невизначеності. Невизначеність може мати різний характер. Так, невизначеними є сплановані дії хакерів, які скеровані на зменшення ефективності систем захисту; невизначеність може стосуватися ситуації ризику, в якій система управління інформаційної мережі, що приймає рішення по застосуванню системи захисту, здатна встановлювати не тільки усі можливі результати рішень, але й вірогідність можливих умов їх появи. Умови проектування впливають на прийняття рішень підсвідомо, незалежно від дій суб'єкта, що приймає рішення. Застосування теорії ігор в області моделювання процесів прийняття рішень має різні підходи, які в наступний час не систематизовані а інколи і вступають в протиріччя між собою. У зв’язку з цим, аналіз підходів моделювання процесів прийняття рішень при проектуванні систем захисту інформації та обґрунтування класифікації таких підходів, *є актуальними науковими завданнями*.

Аналіз останніх досліджень і публікацій дає змогу дійти висновку, що сучасні методичні підходи розрізнені, неповні, а у деяких випадках суперечливі. Так, використання математичного аналізу [1] дає змогу обґрунтувати лише часткові данні класифікації моделей теорії ігор такі як, кількість зацікавлених сторін та кількість коаліцій дій гравців. Математичні моделі аналізу [2] розкривають тільки моделі за результатами гри, за характером та об’ємом інформації, в залежності від кількості можливих стратегій. Джерело [3] розкриває моделі за кількістю коаліцій дій гравців, за виграшем гри, за характером отримання інформації, за кількістю стратегій. Автори [4] розкривають тільки класичні кооперативні ігри, не вдаючись до їх місця у загальній теорії ігор. Автори [5] у загалі надають приклади безкінцевих антагоністичних ігор не розкриваючи класифікації математичних підходів теорії ігор. Автор [6] розкриваючи моделі статистичних та динамічних ігор і будуючи математичні перетворення в інтересах моделювання нападів на інформацію, зовсім не визначив місце і роль математичних моделей теорії ігор в аналізі систем захисту інформації. Надаючи обґрунтування доцільності застосування теорії ігор для моделювання процесів нападу на інформацію автор [6] пропонує такі перетворення тільки для 2-х гравців, що є частковим прикладом коаліційної гри, а не питання розгляду роботи системи захисту інформації у цілому. Особливо це важливо при розгляді питань аналізу систем захисту інформації під час проектування.

Для проведення аналізу процесів прийняття рішення розробнику необхідно мати чітку уяву місця своїх досліджень в предметній області. Пропонуючи основні результати досліджень в області захисту інформації необхідно відштовхуватися від зрозумілих посилань на місце аналітичних

моделей прийняття рішень в процесі моделювання роботи систем захисту інформації.

Література:

1. Оуен. Г. Теория игр / Г. Оуен. — М.: 1971. — Мир. — 230. с.
2. Вентцель Е.С. Элементы теории игр / — М.: 1961. — Физматгиз. — Вип. 32. — 72 с.
3. Петросян Л.А. Теория игр / — М.: 1998. — Вища школа. — 304 с.
4. Дюбин Г.Н. Введение в прикладную теорию игр / — М.: 1981. — Наука. — 336 с.
5. Воробьев Н.Н. Бесконечные антагонистические игры / М.: 1993. — Вища школа. — 505 с.

УДК 621.376.54

Д.Л. Фігура, В.П. Новіков

Державний університет телекомунікацій

ОБҐРУНТУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ СИСТЕМ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Розвиток інформаційних технологій, глобальної мережі Інтернет, а також стрімке зростання обчислювальних можливостей комп'ютерних систем, швидке зростання обсягів оброблюваних даних у сучасних системах автоматизації банку (САБ), поява нових форм електронних послуг, запропонованих САБ, висувають нові вимоги до надійності і забезпеченню безпеки у внутрішньоплатіжних банківських системах (ВПС).

Поява й активізації загроз в інформаційній сфері, передусім загроз від ведення інформаційних війн, суттєво підвищує роль і значення інформаційної безпеки в системі національної безпеки України і обумовлює розширення її змісту. Віра та контроль над національними інформаційними комунікаціями у XXI столітті може призвести до втрати національної незалежності. Цілісну картину всіх можливостей захисту створити досить важко, оскільки ще немає єдиної теорії захищених систем. Існує багато підходів і точок зору щодо методології побудови їх. Докладається багато зусиль як у практичному, так і в теоретичному плані, використовуються останні досягнення науки, передові технології. Займаються цими проблемами провідні фірми з виробництва комп’ютерів і програмних забезпечень, провідні університети та інститути.

Нинішні умови функціонування банківської системи України характеризуються значним розширенням обсягів і структури платіжного обороту, ускладненням розрахунків завдяки розмаїттю їх видів і форм, появою електронних грошей, високим рівнем автоматизації розрахунків, створенням значного за обсягами міжбанківського ринку, що функціонує в межах створеної Національним банком України системи електронних платежів. У зв’язку з цим важливого значення набувають проблеми безпеки функціонування платіжних

систем, організації системи захисту інформації та реалізації відповідної концепції управління фінансовими і нефінансовими ризиками, що притаманні платіжним системам.

Міжнародна платіжна система здійснює свою діяльність на території двох і більше країн та забезпечує переказ грошових коштів у межах цієї платіжної системи. Сьогодні міжнародні платіжні системи — невід'ємний елемент і сервіс банків. Захист інформації у трансакціях при здійсненні міжнародних грошових переказів засобами платіжних систем є однією з основних умов їхнього функціонування. При побудові захисту національних і міжнародних платіжних систем у комплексі використовуються правові, організаційні, технічні, апаратно-програмні та криптографічні засоби і методи захисту інформації. Вони спрямовані на забезпечення захисту інформації від неправомірного доступу, знищення, модифікації, блокування, копіювання, розповсюдження, порушення конфіденційності та інших неправомірних дій відносно до інформації.

Обов'язком служб інформаційної безпеки банків є: реалізація політики забезпечення захисту інформації в національних і міжнародних платіжних системах, моніторинг виконання вимог щодо забезпечення захисту інформації, виявлення інцидентів і реагування на них, удосконалення системи.

Обов'язком банку є також інформування користувачів міжнародної платіжної системи про правила виконання переказів і забезпечення захисту інформації з метою підвищення рівня інформованості користувачів та успішного виконання операцій у системі.

УДК 004.681

В.О. Хорошко, Ю.Є. Хохлачова

Національний авіаційний університет,hohlachova@gmail.com

ЗАХИСТ ІНФОРМАЦІЇ АВТОМАТИЗОВАНИХ СИСТЕМ

Інформаційна безпека відіграє важливу роль у забезпеченні життєво важливих інтересів будь-якої держави. Створення розвинутого і захищеного інформаційного середовища є необхідною умовою розвитку суспільства та держави. Останнім часом в світі відбуваються якісні зміни у процесах управління на всіх рівнях, обумовлені інтенсивним впровадженням сучасних інформаційних технологій, що тягне за собою можливість втручання в їх роботу.

Саме тому, останнім часом в суспільстві все більше і більше уваги приділяється проблемам захисту інформації та пошуку шляхів її вирішення.

Особливе занепокоєння викликає практично стихійний розвиток та використання мережі Інтернет, що створює сприятливі передумови для використання її можливостей зловмисниками. Широке впровадження в захищених інформаційно-комунікаційних системах України комплексної

системи захисту інформації дає змогу захистити важливу для держави інформацію.

Для підвищення ефективності захисту необхідно розробити системний підхід до цієї проблеми, який полягає у проведенні ряду заходів за такими основними напрямками:

- визначення порядку проведення робіт і надання послуг у галузі безпеки інформації;
- розробка нормативних документів, що визначають етапи життєвого циклу захищених інформаційних систем, критерії оцінки рівня захищеності інформації, ефективності системи захисту;
- підготовка і перепідготовка кадрів для роботи в сфері інформаційної безпеки;
- створення вітчизняної інфраструктури розробки, виробництва, впровадження та експлуатації засобів захисту інформації.

Тому можна зробити висновок: рішення задач зберігання і обробки інформації в системах на сьогоднішній день вимагає гнучкого підходу. У сучасних умовах, коли повсякденне життя насичене всілякими технічними засобами діяльності, різними засобами зв`язку, різного роду допоміжними системами, вкрай необхідно розуміти небезпеку виникнення каналів витоку інформації саме через технічні засоби обробки, зберігання та передачу конфіденційного характеру. Біль того, технічні засоби відносяться до найбільш небезпечних і широко розповсюджених каналів витоку інформації.

Як висновок необхідно зазначити, що специфіка територіально рознесених автоматизованих систем, з точки зору їх вразливості, пов`язана в основному взаємодією між її елементами.

Інформація в автоматизованих системах — це сукупність усіх даних і програм, які використовуються в автоматизованих системах незалежно від способу їх фізичного та логічного подання. Захист інформації — сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння шкоди інтересам власника чи автоматизованій системі, які користуються інформацією.

Об'єктами захисту є інформація, що обробляється в АС, права власності цієї інформації, що обробляється в АС, права власника цієї інформації та власників АС, права користувачів. Захисту підлягає будь-яка інформація в АС, необхідність захисту якої визначається її власником або чинним законодавством.

Захист інформації автоматизованих систем забезпечується шляхом:

- додержання суб'єктами правових відносин норм, вимог і правил організаційного та технічного характеру щодо захисту обробленої інформації;
- використання засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку та автоматизованих систем в цілому, засобів захисту інформації, які відповідають встановленим вимогам щодо її захисту;

- перевірки відповідності засобів обчислювальної техніки програмного забезпечення, засобів зв'язку та автоматизованих систем у цілому встановленим вимогам щодо захисту інформації;
- здійснення контролю щодо захисту інформації.

Результатами порушення захисту інформації в автоматизованих системах можуть бути: витік інформації, втрата інформації, підробка інформації, порушення роботи автоматизованих систем.

Інформаційною системою з безпеки має управляти головний спеціаліст з безпеки, який повинен звітувати безпосередньо раді керівників і мати повну незалежність. Звіти повинні охоплювати кожну фазу життєвого циклу системи.

Існує два основних підходи до аналізу "вразливих" місць і загроз системи: кількісний та якісний підходи до оцінки ризиків втрати інформації.

Кількісний підхід до оцінки ризику — кожен рівень доступності ризику потенційних збитків обчислюється як результат вартості окремого збитку, помноженого на вірогідності його виникнення. При застосуванні кількісного підходу може бути складно оцінити кожен випадок збитку та вірогідність його виникнення. При застосуванні кількісного підходу може бути складно оцінити кожен випадок збитку та вірогідність його виникнення, а також необхідно передбачити майбутні події.

Якісний підхід до оцінки ризику показує вразливі місця та загрози системи, суб'єктивно зростаючи їх у порядку значущості для сукупної доступності компанії ризику потенційних збитків.

Інформаційні ресурси є основним чинником економічного зростання, тому в конкурентному середовищі інформація потребує захисту. На сьогодні існує теоретичний матеріал та розроблені практичні заходи захисту інформації в КІСБО. Проте не можна вважати цю проблему вирішеною. У подальшому слід приділити увагу дослідженню проблем розмежування доступу до функції і файлів системи організаційної структури КІСБО з урахуванням основних принципів внутрішнього контролю, розробці рекомендацій щодо розмежування доступу на підприємствах різних галузей і використанням різних програмних продуктів. Потребують дослідження проблеми юридичної доказовості створених електронних документів, а також контролю інформації в умовах комп'ютерного способу обробки та інші.

УДК 004.056

Я. В. Шестак, А.Г. Оксиюк, д.т.н.

Киевский национальный университет имени Тараса Шевченка,
lucenko.y@ukr.net

ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ АНАЛИЗА ДАННЫХ МОНИТОРИНГА НЕСКОЛЬКИМИ СПОСОБАМИ

В целях решения задачи обнаружения компьютерных атак может быть использован достаточно широкий круг методов сбора и анализа данных мониторинга. При этом каждый из методов имеет свои достоинства и недостатки, выражающиеся в различии качественных характеристик,

требованиях к вычислительным ресурсам, сложности реализации и времени срабатывания. Очевидно, что применение в одной системе обнаружения атак (СОА) нескольких методов может компенсировать их недостатки и, тем самым, позволит добиться лучших результатов по точности детектирования атак по сравнению с системами, использующими только один из методов анализа.

В целом принято выделять две группы методов обнаружения компьютерных атак: основанные на знаниях и основанные на поведении. Если СОА использует информацию об уже известных атаках и способах их осуществления, то она относится к системам, основанным на знаниях. Если же для обнаружения атаки система использует информацию о закономерностях (профиле) поведения системы, в которой осуществляется мониторинг, то она относится к системам, основанным на поведении.

Воплощением методов, основанных на знаниях, является сигнатурный анализ, также широко применяемый в антивирусных средствах. Любой компьютерной атаке соответствует определенный сетевой трафик (для удаленной атаки) или поток системных событий (для локальной атаки), фиксируемый средствами аудита и мониторинга. Данная информация однозначно отличает каждую атаку от любой другой атаки или штатного поведения контролируемой системы и называется сигнатурой. Так, например, сигнатурный анализ был признан наиболее эффективным в случаях атомарных или подобных им по проявлениям атак, когда деструктивное воздействие заключается или завершается одним ключевым сетевым пакетом, особенности которого достаточно просто выявить для формирования сигнатуры. В процессе сигнатурного анализа активность в сети, данные системного аудита или данные других индикаторов сравниваются с содержимым базы данных сигнатур уже известных атак, и при совпадении подается сигнал тревоги.

Описанный подход является наиболее простым в реализации, обладает высокой точностью и быстродействием при обнаружении атак. Однако его существенный недостаток — необходимость постоянного пополнения используемой базы сигнатур.

Методы, основанные на поведении, были разработаны для компенсации описанного недостатка. Их воплощением является статистический анализ. В данном случае поведение системы характеризуется набором показателей, временные ряды значений которых собираются датчиками системы мониторинга, при этом периодичность сбора значений и их состав могут быть выбраны, исходя из специфики контролируемой системы.

В дальнейшем значения показателей сравниваются с выявленными ранее значениями, соответствующими штатной работе — профилем. В случае несовпадения фиксируется факт атаки.

Задача составления профиля штатного поведения является достаточно трудоемкой и к настоящему времени не имеет универсального решения. Дополнительной трудностью является также то, что сам профиль с течением времени может изменяться. Кроме того, статистическим методам свойственна высокая вероятность ошибки второго рода. В последнее время среди поведенческих методов, в той или иной мере основанных на измерении и

рассмотрении статистических значений, в особый класс выделяют интеллектуальные методы анализа данных, основным достоинством которых является способность к самообучению, т.е. автоматизации процессов формирования и адаптации с течением времени профилей поведения контролируемых систем. Статистический и нейросетевой (определенный вид параметрических статистических методов) методы выявления аномального поведения в локальной сети характеризуются необходимостью некоторого временного периода на формирование профилей. При этом для нейросетевого подхода преимуществом является автоматическое формирование профилей поведения (которыми, по сути, являются сами обученные нейронные сети), а для статистического — меньшая, по сравнению с нейросетвым, ресурсоемкость.

Таким образом, сигнатурные и поведенческие методы обладают взаимоисключающими достоинствами и недостатками, поэтому их совместное применение в составе единой СОА сулит существенные преимущества.

Важнейшую роль при использовании нескольких методов анализа приобретает выбор и применение того или иного метода принятия решений об обнаружении компьютерных атак. Причем указанная проблема имеет два уровня: принятие решения в рамках одного метода анализа (сигнатурного или поведенческого) и принятие решения при одновременном использовании нескольких методов, особенно если их результаты расходятся.

В настоящее время наиболее распространенным методом принятия решений является подход на основе правил, по сути превращающий систему обнаружения атак в продукционную экспертную систему. Также могут быть применены методы анализа иерархий, интеллектуальные методы и др. Особо стоит отметить перспективность интеллектуальных методов, в частности, искусственных нейронных сетей, главным преимуществом которых является способность самостоятельно формировать и адаптировать свое представление о нормальном поведении системы, чтобы в последующем фиксировать отклонения от него, а также способности решать задачи распознавания ситуаций, в которых следует отдавать предпочтение определенному методу обнаружения атак. Таким образом, потенциально применение нейросетей позволит решить, как задачу автоматизации формирования и адаптации профилей, так и задачи принятия согласованных решений и автоматизации формирования сигнатур новых обнаруженных атак.

Литература:

1. *Райан Д., Ли М-Д., Миккулайнен Р.* Обнаружения атак с помощью нейросетей. Перевод *А.В. Лукацкий* (НИП «Информзащита»), Ю.Ю. Цаплев (НИП «Информзащита»).— http://www.infosec.ru.

2. *Милославская Н.Г.., Толстой А.И.* Интрасети: обнаружение вторжений. М.:ЮНИТИ-ДАНА. 2001. — 587 с.

3. *Лукацкий А.В.* Обнаружение атак. — 2-е изд., СПб. БХВ-Петербург. 2003. — 608 с.

4. *Бейс Р.* Введение в обнаружение атак и анализ защищенности. Перевод *А.В. Лукацкого, Юрия Цаплева,* (НИП "Информзащита) — http://bugtraq.ru/library/books/icsa/.

УДК 621.397.2

Н.В. Цепа, В.С. Наконечний

Державний університет телекомунікацій

РОЗРОБКА МЕТОДИКИ КОНТРОЛЮ СТАНУ КАНАЛУ СИСТЕМ РАДІОЗВ'ЯЗКУ ПРИ ВПЛИВІ НАВМИСНИХ ЗАВАД

З метою підвищення ефективності функціонування мобільних компонентів систем зв'язку планується широке використання в їх складі засобів і систем радіозв'язку (СРЗ). Це дозволить розв'язати існуючі проблеми по безперервності та стійкості управління вже найближчим часом і відкриває подальші перспективи на поліпшення технічних характеристик системи зв'язку вцілому.

Одними з основних факторів, що впливають на якість радіозв'язку є завмирання сигналів, які виникають внаслідок багатопроменевого розповсюдження радіохвиль, та навмисні завади.

При передачі сигналів багатопроменевими каналами зв'язку широко використовується метод модуляції, що має назву ортогональне частотне розділення з мультиплексуванням (Orthogonal Frequency Division Multiplexing OFDM). Основними перевагами даного методу модуляції є висока стійкість до селективних завмирань, а також висока частотна ефективність.

При побудові СРЗ із OFDM велика увага приділяється питанням оптимізації алгоритмів формування та обробки сигналів, які дозволяють підвищити показник якості функціонування при заданих обмеженнях на інші показники.

Актуальність теми. Методи оптимізації OFDM-сигналів, удосконалення алгоритмів їх формування та обробки є об'єктом інтенсивних теоретичних досліджень протягом останніх років. Однак більшість теоретичних результатів, а також методів, впроваджених в існуючі СРЗ, що використовують модуляцію OFDM, одержані з метою підвищення швидкості передачі інформації при обмеженнях на енергетику та ширину смуги робочих частот (підвищення частотної ефективності системи). Для систем широкосмугового радіодоступу така постановка завдання обумовлена, в першу чергу, комерційним призначенням цих систем та прагненням розробників засобів зв'язку забезпечити високошвидкісний безпровідний доступ до мережі Internet якомога більшій кількості користувачів одночасно. Для систем зв'язку, де, як правило, інформаційне навантаження на напрямках зв'язку є відомим, більш актуальною є задача підвищення енергетичної ефективності при обмеженнях на пропускну спроможність, смугу пропускання та достовірність.

Відомі методи підвищення енергетичної ефективності систем та засобів радіозв'язку одержані для випадку передачі інформації по гаусівському каналу

без пам'яті. Наявність у каналі селективних завмирань і навмисних завад не дозволяє при прийнятній складності реалізації відомих алгоритмів передачі дискретних повідомлень досягти тієї ж ефективності використання реальних каналів зв'язку, що й ідеального гаусівського півнеперервного каналу.

Отже, завдання підвищення енергетичної ефективності СРЗ в умовах багатопроменевого поширення радіохвиль і активної радіоелектронної боротьби є актуальним і має не тільки теоретичне, але і велике прикладне значення для забезпечення необхідного рівня бойової готовності за рахунок підвищення своєчасності, вірогідності та прихованості бойового управління.

Таким чином, у доповіді вирішується актуальна *наукова задача*, що має важливу наукову та технічну спрямованість при створенні перспективних цифрових систем радіозв'язку — *розробка методики вибору оптимальних значень параметрів OFDM-сигналу в залежності від стану каналу зв 'язку в умовах частотно-селективних завмирань та навмисних завад для підвищення енергетичної ефективності засобів радіозв'язку.*

УДК 004.7(045)

О. К. Юдін, Р. В. Зюбіна

Національний авіаційний університет, kszi@ukr.net

КОНЦЕПЦІЯ ВПРОВАДЖЕННЯ ХМАРНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

В сучасному світі тема хмарних технологій набуває все більш широких обертів. Подальшому розвитку і шляхам побудови нової інфраструктури країни, новим технологічним рішенням реалізації ІТ систем, присвячуються сучасні науково-практичні конференції, ведуться дослідження та публікуються огляди. Чинники і технологічні вимоги, що можуть бути визначені, як ключові для подальшого розвитку і становлення ефективних й інноваційних хмарних служб для використання інформаційних ресурсів можна виділити на наступні:

1. Безпека

- Користувачам хмари потрібні гарантії, що інформація, яка зберігається в хмарі знаходиться в безпеці і ризик її втрати неможливий. Це справедливо як для державних підприємств, так і для приватних. Для досягнення потрібного рівня безпеки, провайдер має виконати комплекс заходів захисту.

Боротьба з несанкціонованими діями

Незаконна діяльність в хмарі, така як цифрова злочинність, фальсифікація і злом — становить загрозу як користувачам хмари, так і постачальникам послуг.

Конфіденційність

Користувачам хмари необхідні гарантії того, що їх конфіденційна інформація, яка зберігається, обробляється і передається в хмарі, не буде використана або розкрита провайдером в корисних цілях.

- Провайдери мають встановити політику конфіденційності, яка відповідатиме специфіці функціонування послуг, які вони надають і бізнес-моделі, яку вони використовують.

2. Функціональна сумісність

Мобільність даних і цілісне використання взаємодіючих програмних засобів — ключовий фактор для усіх користувачів хмарних технологій.

- Постачальники послуг повинні працювати разом, щоб гарантувати, що функціональна сумісність і портативність вирішуються шляхом відкритого співробітництва і належного використання прийнятих міжнародних стандартів у відповідних випадках.
- Державні органи мають прийняти стандарти для функціональної сумісності і портативності, яка розвивається.

3. Захист інтелектуальної власності

Провайдери хмарних технологій та послуг покладаються на патенти, авторські права та інші форми захисту інтелектуальної власності.

- В законах про інтелектуальну власність треба передбачити та розробити систему захисту і санкції проти незаконного привласнення і використання інформації, що циркулює в хмарі.

4. Удосконалення нормативної бази

Національні уряди впроваджують, або розробляють, іноді суперечливі правові зобов’язання відносно використання даних користувача і послуг, що надають провайдери. Ці суперечливі зобов'язання перешкоджають нововведенню і підривають споживчу довіру до хмари.

5. Сприянні вільній торгівлі

- Використання хмарних технологій передбачає співпрацю через національні кордони, і їх успіх залежить від доступу до світових ринків.

Отже, використання хмарних технологій має широкий спектр переваг, однак досі залишається відкритим питання нормативно-правового врегулювання взаємодії постачальника послуг та користувача.

В українське законодавство мають бути внесені зміни з обов’язковим врахуванням подальшого розвитку хмарних технологій в країні і світі.

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

Наукові доповіді та тези учасників
науково-технічної конференції
12-13 березня 2015 року

Виготовлювач:
ФОП Довбня Сергій Якович
Єдиний державний реєстр юридичних
та фізичних осіб-підприємців
серія АГ № 005738 2013 року
Послуги з технічного захисту інформації ліцензія: серія АЕ № 271465 2014 року

Підписано до друку 07.04.2015 р. Зам. № 59п
Формат 60х84/8. Папір 80 г/м^2.
Друк. арк. 19,50. Ум.-друк арк. 18,14. Обл.-вид. арк. 12,75.
Тираж 100 примірників.

Надруковано ТОВ «НікС»
з електронного носія виготовлювача
02002, м. Київ, вул. Флоренції, 1/11
Тел./факс (044)516-8430 541-1549
e-mail: publish@nics.com.ua www.nics.com.ua
Свідоцтво про внесення до Державного реєстру
суб'єкта видавничої справи ДК № 938 від 04.06.2002