МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

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

РАДА МОЛОДИХ ВЧЕНИХ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. БЕЗПЕКА ТА ЗВ'ЯЗОК

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

Частина І

20 квітня 2017 р.

м. Дніпро

УДК [004+621.39](06)
І 74
ББК 32.973

Оргкомітет конференції:

Голова:	Декан факультету інформаційних технологій, д.т.н., професор Алексєєв М.О.
Заступник голови:	Голова ради молодих вчених факультету інформаційних технологій Мєшков В.І.
Члени оргкомітету:	д.т.н., професор Корнієнко В.І. к.т.н., доцент Флоров С.В. к.т.н., доцент Школа М.І. ст. викл. Войцех С.І. ас. Масальська О.О.

І 74

Інформаційні технології. Безпека та зв’язок: Матеріали всеукр. наук.-практ. конф. – Дніпро: Державний ВНЗ «Національний гірничий університет», 2017. – 16 с. – Частина І (укр. м., рос. м., англ. м.).

Викладено тези доповідей учасників XI Всеукраїнської науково-практичної конференції «Інформаційні технології. Безпека та зв’язок», яка відбулася у Державному ВНЗ «Національний гірничий університет» 20 квітня 2017 року. На конференції було розглянуті найбільш актуальні проблеми розвитку інформаційних технологій, безпеки та зв’язку в Україні та шляхи їх вирішення.

УДК [004+621.39](06)
ББК 32.973

ЗМІСТ

Секція «Кібербезпека»

Секція «Кібербезпека»

Голова секції: д.т.н., професор кафедри безпеки інформації та телекомунікацій Корнієнко В.І.
Секретар секції: асистент кафедри безпеки інформації та телекомунікацій Мєшков В.І.

УДК 004.052.42+004.383

ВРАЗЛИВОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СЕРВЕРНОГО ОБЛАДНАННЯ

Колісніченко Дмитро Вадимович
Керівник – співавтор: Масальська Олена Олександрівна
Державний ВНЗ «Національнальний гірничий університет»,
http://bit.nmu.org.ua/, SDKolisnichenko@gmail.com

В роботі розглянуто програмне забезпечення, яке встановлене на термінальному серверному обладнанні. Проаналізовані вразливості та недоліки цих систем. Розроблені рекомендації щодо мінімізування вказаних вразливостей.

Ключові слова: Вразливість, програмне забезпечення, MS SQL сервер.

ВСТУП

Цілісність даних слід розглядати як основну проблему безпеки інформації. У кожній версії програмного забезпечення є свої засоби безпеки інформації. Програмний засіб має унікальні вимоги, середу виконання та фізичне розташування. Деякому програмному забезпеченню потрібний мінімальний захист інформації, тоді як іншим локальним додаткам чи додаткам, які розгорнуті через інтернет, можуть вимагатися суворі заходи безпеки інформації, разом з постійним моніторингом та контролем.

Навіть якщо програмний засіб розроблений бездоганно, в міру розвитку шкідливого програмного забезпечення, можуть з'явитися нові вразливості. Тому розробникам цих програмних продуктів слід своєчасно реагувати на нові вразливості.

Деякі вразливості залежать не тільки від розробників цих систем, але і від факторів управління цією системою:

1. Складність паролів, які були задані адміністраторами системи;
2. Привілеї для користувачів;
3. Системи безпеки, встановленні на даному обладнанні;
4. Адміністрування системи в цілому.

В цій роботі розглянуто системи, які встановленні на серверному обладнанні, а саме «Windows Server 2008» та «MS SQL Server 2008», та наведені основні недоліки та вразливості цих систем [1].

ТЕОРЕТИЧНІ ДАНІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Microsoft SQL Server - система керування базами даних. Програмне забезпечення використовує мову запитів - Transact-SQL, створений спільно з Microsoft та Sybase. Використовується для роботи з базами даних розміром від персональних до великих баз даних масштабу підприємства.

MS SQL Server містить великий набір інтегрованих служб з аналізу даних. Доступ до даних, розташованих на MS SQL Server, можуть отримати будь-які додатки, розроблені за допомогою технології .Net і середовища розробки Visual Studio, а також додатки пакета Microsoft Office. Для конфігурації, управління та адміністрування всіх компонентів Microsoft SQL Server використовується інструментарій утиліт SQL Server Management Studio. У ній існує підтримка ряду компонент і засобів по створенню і управлінню базами даних, засобів аналітичної обробки даних (Analysis Services), засобів звітності (Reporting Services), а також безліч засобів, що спрощують розробку додатків [2].

Windows Server - серверна операційна системи від Microsoft. Система являє собою захищену і легко керовану платформу для розробки і надійного розміщення веб-додатків і служб. Операційна система Windows Server 2008 надає адміністраторам можливості для управління серверами і мережевою інфраструктурою, що дозволяє зосередитися на найважливіших потребах організацій. Розширені можливості створення сценаріїв і автоматизації завдань, такі як середовище Windows PowerShell, дозволяють автоматизувати стандартні завдання адміністраторів. Операційна система дозволяє виконувати установку і управління на основі ролей, що полегшує завдання управління та забезпечення безпеки різних ролей серверів в рамках підприємства. Можлива установка тільки необхідних ролей і можливостей [3].

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ СЕРВЕРНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Розглянемо вразливості та недоліки Windows Server 2008. В 2016 році була виявлена вразливість в реалізації протоколу Network Basic Input/ Output System (Net Bios).

Net Bios – це протокол для роботи в локальних мережах, розроблений у вигляді інтерфейсу.

Протокол Net Bios використовується на платформах Windows. Критична вразливість отримала назву «Bad Tunnel» – ця вразливість

дозволяє зловмисникам повністю контролювати мережевий трафік жертви.

«Bad Tunnel» дозволяє зловмисникам контролювати не тільки HTTP та HTTPS запити, але і всю мережеву активність операційної системи, наприклад, втручатися в завантаження системних оновлень та в процес отримання списків сертифікатів системи. Вразливі всі версії програмного забезпечення Windows. Перенаправлення трафіка жертви може здійснюватися за допомогою підробленого WPAD – файлу (Web Proxy Auto Discovery) або ISATAP – серверу (Intra Site Automatic Tunnel Adressing Protocol).

WPAD – метод, який використовується клієнтами для визначення місця (URL) розташування конфігураційного файлу з використанням технології DHCP або DNS.

ISATAP – протокол, що дозволяє передавати між мережами IPv6 пакети через мережі IPv4 [4].

Наступна вразливість має ім'я «Freak». Вразливість дозволяє зловмисникам перехоплювати всі дані, що передаються зашифрованими з'єднаннями HTTPS. Найчастіше такою технологією користуються платіжні системи, сайти банків.

Як стало відомо, дана вразливість виникла через обмеження на експорт криптографічного продукції, діючих в США на момент розробки протоколу.

Розглянемо, критичні вразливості на MS SQL Server 2008. Хоча SQL Server включає різноманітні механізми захисту, система містить функції, якими можна скористатися для шкідливих цілей. Кожен компонент, який відкриває доступ до будь-яких даних, може бути джерелом небезпеки при невірної реалізації. Потенційному порушнику необхідно отримати доступ до MS SQL з роллю «Адміністратор бази даних», а це може легко статися якщо:

1. Пароль стандартного облікового запису «sa» в SQL Server порожній або може бути легко підібраний, що часто зустрічається, коли система управління базою даних використовується в тестової експлуатації, або як платформа для розробників;
2. Неправильно призначені ролі користувачів в самій системі управління базою даних: обліковий запис звичайного користувача системи управління базою даних володіє роллю «Власник бази даних», або роллю «Адміністратор бази даних»;
3. Пароль деякого облікового запису, що входить до групи «Адміністратори», пустий чи може бути легко підібраний або визначений (завдання отримання доступу до сервера, знаючи пароль адміністратора, на перший погляд може здатися дивною, але, наприклад, якщо до сервера дозволено з'єднання лише до портів MS SQL, то цей спосіб дозволяє виконувати команди операційної системи).

Потім потенційний порушник може виконати розширену процедуру «xp_cmdshell», вказавши їй, як параметр команду операційної системи, яка створює користувача і включає його в групу "Адміністратори", щоб отримати повний доступ до сервера, на якому встановлена система управління базою даних [2].

ВИСНОВОК

Безпека є важливою характеристикою для будь-якого продукту і будь-якого підприємства. Дотримуючись простих рекомендацій, можна уникнути багатьох вразливостей в безпеці.

Успішно проведена атака на програмне забезпечення може заподіяти повну втрату інформації.

Для того що б мінімізувати шкідливу активність на публічних пристроях, потрібно використовувати такі методи:

1. Необхідно встановити брандмауер між сервером та інтернетом;
2. Необхідно розділити мережу на зони безпеки, розділені брандмауерами. Заблокувати весь потік даних, після чого дозволити тільки необхідний;
3. Необхідно на зовнішніх серверах мережі повинні бути відключені всі непотрібні протоколи, включаючи NetBIOS і SMB;
4. Необхідно запускати служби SQL Server з мінімально можливими дозволами;
5. Завжди призначайте надійний пароль для облікового запису.

Система безпеки в програмному забезпечені постійно вдосконалюється. Однак, такі загальні загрози безпеки, як крадіжка даних існують незалежно від самого програмного забезпечення [4].

Отже, в цій роботі розглянуті системи, які встановленні на термінальному серверному обладнанні, виконаний аналіз вразливостей та наведені методи мінімізування вразливостей в програмному забезпеченні.

ЛІТЕРАТУРА

1. Безпека SQL Server [Електронний ресурс]: https://msdn.microsoft.com/ru-ru/library/ bb669074(v=vs.110).aspx;
2. Майк Хотек Реалізація і обслуговування Microsoft SQL Server 2008.- Русская Редакция-2011.- 576 с;
3. Технічний огляд Windows Server [Електронний ресурс]:http://man.odn.org.ua/Page-5/Win2008_Review/page.htm;
4. Критичні вразливості Windows Server [Електронний ресурс]: https://habrahabr.ru/ company/pt/blog/304842/;
5. Безпека інформації [Електронний ресурс]: https://msdn.microsoft.com/ru-ru/library /ms144228.aspx.

УДК 65.012.8:621.391.6

ЗАХИСТ МОВНОЇ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ЗНЯТТЯ ПРИ ПЕРЕГОВОРАХ ДВОХ ОСІБ

Швачка Р.С., Науковий керівник: Школа М.І.
Державний ВНЗ «Національнальний гірничий університет»,
http://bit.nmu.org.ua/ E-mail: roma-nius@yandex.ru

Дана робота присвячена одній з найбільш поширених завдань в галузі захисту інформації - аналізу і проектування системи безпеки інформації від несанкціонованого знімання при переговорах двох осіб. Розглядаються декілька способів захисту інформації від витоку і несанкціонованого знімання, зокрема, проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням портативних електронних пристроїв перехоплення інформації (заставних пристроїв).

Ключові слова - захист мовної інформації, передавач акустичного (мовного) сигналу по ІЧ – каналу, захист інформації за допомогою IrDA.

З найдавніших часів людська мова — найбільш поширений метод обміну інформацією між людьми, тому спроби перехоплення мовної акустичної інформації давно вже використовуються зловмисниками. Особлива їх зацікавленість в отриманні мовної інформації пояснюється тим, що мова досить часто містить відомості конфіденційного і навіть секретного характеру. Саме інформація є одним із найважливіших засобів розв'язання проблем та завдань, як на державному рівні, так і на рівні комерційних організацій і окремих осіб.

В повітряні (прямі акустичні) технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря. Для перехоплення акустичних сигналів в якості датчиків засобів розвідки використовуються мікрофони. Сигнали, що надходять з мікрофонів або безпосередньо записуються на спеціальні портативні пристрої звукозапису, або передаються з використанням спеціальних передавачів в пункт прийому, де здійснюється їх запис.[1]

До технічних заходів з використанням пасивних засобів належать:

- контроль і обмеження доступу на об'єкти ТЗПІ і виділені приміщення,
- локалізація випромінювань і розв'язування інформаційних сигналів,
- установка спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалення, водопостачання та каналізації, що мають вихід за межі контрольованої зони,
- установка в ланцюгах електроживлення ТЗПІ, а також у лініях освітлювальної і розеткової мереж виділених приміщень протизавадних фільтрів типу ФП.

До технічних заходів з використанням активних засобів відносяться:

- просторове зашумлення. Просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних перешкод з використанням засобів створення прицільних перешкод,
- лінійне зашумлення. Лінійне зашумлення ліній електроживлення, Лінійне зашумлення сторонніх провідників і з'єднувальних ліній, що мають вихід за межі контрольованої зони,
- знищення закладних пристроїв. Знищення закладних пристроїв, підключених до лінії, з використанням спеціальних генераторів імпульсів.[2]

Одним із останніх сучасних винаходів в області радіотехніки є перетворення корисного акустичного сигналу в інфрачервоний діапазон. Інфрачервоний канал має безліч переваг:

- не вимагає для свого функціонування дротових з'єднань;
- висока конфіденційність зв'язку, так як передача здійснюється вузьким променем при повній відсутності бічних випромінювань;
- недорога вартість радіокомпонентів;
- відсутність необхідності у дозволах на використання радиочастотного спектру.

До складу передавача акустичного (мовного) сигналу по ІЧ – каналу входять наступні елементи:

- мікрофон,
- підсилювач,
- аналого-цифрової і цифроаналоговий перетворювач,
- головний телефон,
- КодеК (шифратор - дешифратор),
- світлодіод,
- фотодіод.

Корисний акустичний сигнал від опонента А надходить на мікрофон і попередньо посилюється. Перед цим відбувається частотна корекція сигналу з метою підвищити завадостійкість, так як нам не потрібен весь частотний діапазон. Так як нам потрібно надалі зашифрувати сигнал, необхідно провести його оцифровку. Перетворення звичайної безперервної синусоїди в цифровий сигнал з дискретними значеннями 0 і 1 відбувається в мікросхемі аналого-цифрового перетворення (АЦП). Потім в кодеку відбувається кодування сигналу, після перетворення в АЦП зіставляють які-небудь величини, свого роду шифри. Після відбувається посилення оцифрованого сигнала і подача його на випромінюючий світлодіод.

Закодований цифровий сигнал від опонента приймається на фотодіод, посилюється, розкодовується, проходить цифро-аналогове

перетворення, посилюється і подача його на головний телефон.

З аналізу загроз безпеки інформації, цілей і завдань її захисту випливає, що досягти необхідного рівня захищеності можна тільки за рахунок комплексного використання існуючих методів і засобів захисту.

ПЕРЕЛІК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Герасименко С. А. Основи захисту інформації: навчальний посібник / В. О. Герасименко. – М: Академія, 2006. – 540 с.

2. Акустичний канал: методи знімання інформації [Електронний ресурс] / Російською – Антена.-2010. – Режим доступу: http://www.razvedka.ru/catalog/580/599/9408.htm

УДК 004

ЗАХИСТ КОРПОРАТИВНОЇ МЕРЕЖІ TITAN BRICK

Гасімов Фархад Мікель Огли, Єлізаров Анатолій Борисович
Національний Авіаційний Університет та nau.edu.ua, farkhadgas1995@gmail.com, a_e_l@rambler.ru

У ході роботи було проаналізовано основні типи атак на комп'ютерні системи, способи боротьби з ними та статті кримінального кодексу законодавства України під які підпадають кіберзлочинці. У результаті аналізу було розроблено план для запобігання основним типам атак та пам'ятку для роботи з персоналом, задля запобігання соціальній інженерії.

ВСТУП

На сьогоднішній день проблема захисту інформаційних ресурсів корпоративних мереж стає все більш актуальною. В ході все більшого проникнення технологій в наше життя і переходу на електронні файли від звичного передавання інформації на папері, комерційна таємниця знаходиться під загрозою з боку зловмисників.

В даній корпоративній мережі компанії TITAN BRICK основною проблемо є те, що офіси віддалені одне від одного, і при деяких офісах існують лабораторії де виготовляють і випробовують нові види цегли. Дані по новим видам цегли постійно повинні відсилатися до головного офісу, де на їх основі роблять розрахунки по економічній вигідності реалізації того, чи іншого продукту. Через це, в цих локальних мережах дуже великий розмір вихідного та вхідного трафіку, що робить завдання захисту більш важким.

ПРИЧИНИ УРАЗЛИВОСТІ МЕРЕЖ

Основна доля витоку інформації з підприємств припадає на злочини, які були вчинені за допомогою використання схем соціальної інженерії. Інформацію не завжди необхідно красти, дуже поширені випадки, коли зловмисники не крали дані з серверів, але знищували їх, чи змінювали інформацію, тим самим завдаючи матеріальні збитки жертвам атаки, в результаті яких жертви ще й втрачали багато часу на відновлення інформації. На сьогоднішній день широке розповсюдження технології Інтернет дозволяє кіберзлочинцям обмінюватися інформацією в режимі реального часу. Вже давно існують потужні міжнаціональні форуми хакерів, де вони обмінюються інформацією про вразливі ресурси, і організують групи для атаки на них. Також потрібно розуміти, що мережа майже ніким не контролюється, і тому зловмисники мають повний спектр можливостей в Інтернеті.

Найбільш актуальним завданням у сфері забезпечення інформаційної безпеки підприємства на сьогоднішній день є чітке розуміння типів атак, які можуть пошкодити мережу, або привести до витоку інформації, володіння потрібними знаннями та інструментами для запобігання витоку даних та розмежовування доступу до важливих елементів системи.

Ще однією причиною уразливості сучасних мереж є використання застарілого програмного забезпечення. Для багатьох програмних продуктів, які мають діло з даними користувача постійно випускають нові версії продукту, де закривають знайденні раніше уразливі місця. Тому, якщо в людини стоїть не оновлене програмне забезпечення, вона дуже підвернена атаці з боку зловмисників, бо хакери вже знають уразливі місця в цій версії програми. Це дозволяє зловмисникам створювати універсальні інструменти для злому. Найбільш доцільним методом захисту є профілактика зломів, бо виявлення хакера після того, як він вже зламав систему і знищив дані, не дасть потрібного результату. Томі найбільш ефективним методом боротьби з зловмисниками буде не допустити їх проникнення в мережу. З розвитком систем зв'язку все більш значущим стає бездротовий зв'язок. Тому на даний момент багато фірм, які забезпечують інформаційну безпеку, уділяють все більше уваги стандартам бездротового зв'язку. Мережні атаки такі ж різноманітні, наскільки різноманітні системи, проти яких вони направлені. Атаки також розділяють за їх цілю, найпростіші атаки такі як, наприклад, DDOS-атака можна перервати простим відключенням серверів, або за допомогою вбудованої утиліти, яка відмовляє в доступі новим користувачам, якщо бачить, що за короткий час на сервер поступає дуже багато запитів, і розуміє, що це так звана атака обмеження доступу.

ТИПИ АТАК НА МЕРЕЖІ

Атака з підбором паролю є однією з найбільш використовуваних. Вона полягає в тому, що злочинник намагається підібрати пароль до аканту адміністратора, або користувача, через грубий підбор паролю, маючи на увазі, що середньо статистичний

користувач не може запам’ятати великі важкі паролі.Для того, щоб отримати пароль, злочинники використовують наступні методи: IP-спуфинг і сниффинг пакетів.

Однією з найстаріших і найпримітивніших типів атак на комп’ютери є атака через пошту, так званий мейлбомбінг.

Існує багато програм для мейлбомбігу, але найпопулярнішими через зловмисників є AutoPMTA та Interspire. Суть атаки на поштову скриньку полягає в тому, що злочинник відсилає критично багато електронних листів, які засмічують папку вхідних листів отримувача, і можуть навіть вивести поштовий сервер з ладу. При цьому програма дає змогу повністю змінювати всі дані відправника, включаючи і IP-адресу. Діє це наступним чином: зловмисник пише текст письма в спеціальній програмі, вказує недостовірні дані відправника, вкрає адресу отримувача і тисне на кнопку почати відправку. На сьогоднішній день багато поштових серверів вже мають спеціальні механізми захисту від поштових атак такого роду, тому їх можна вже не боятися.

Існує два види “шкідливого” программного коду: віруси і "троянські програми". Віруси – це програми, яким прописаний алгоритм дій, направлений на виконання певних дій на кінцевому пристрої користувача.

“Троянські програми”, на відміну від вірусів, направленні на знищення всієї інформації на кінцевому пристрої жертви. Вони отримали свою назву через те, що хакери зазвичай вбудовують ці програми в “нешкідливі” файли, наприклад, ігри, чи офісні програми. “Троянські програми” після потрапляння в систему, намагаються себе не видавати. Вони можуть місяцями сидіти в комп’ютері жертви і ніяк себе не виказувати, і збирати інформацію з пристрою, тому їх часто використовують для промислового шпигунства.

Віруси упроваджуються в інші програми з метою виконання закладеної в них шкідливої функції на робочій станції кінцевого користувача. Віруси вписують свій програмний код в “тіло” програми носія. Сам вірус невеликий – його розмір рідко вимірюється кілобайтами.

Програмні віруси атакують програмне забезпечення комп'ютера і навіть частково змінюють програмний код продукту на свій. Як результат, інфікована програма починає заражати файли, які працюють з нею, що призводить до розповсюдження вірусу по комп’ютеру. Одним з найнебезпечніших вірусів цього типу виявився вірус Chernobyl, який заражає все програмне забезпечення жертви, а потім атакує BIOS комп'ютера.

Аналізатор трафіку, або сніфер (від англ. to sniff — нюхати) — мережний аналізатор трафіку, програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережного трафіку, призначеного для інших вузлів. Сніффер пакетів є прикладною програмою, яка використовує мережеву карту, працюючу в режимі, при кому всі пакети, отримані по фізичних каналах, мережний адаптер відправляє додатку для обробки). Сніффер вміє перехоплювати всі пакети, які передаються через домен по мережі, що атакується.

На сьогоднішній день, в багатьох мережах використовують сніффери для добрих цілей, а саме для аналізу і перехоплення трафіку.

ЕТАП, ЩО ПЕРЕДУЄ АТАЦІ

Перед тим, як розпочати атаку, зловмисники звичайно проводять мережеву розвідку, під час якої шукають слабкі місця в системі інформаційного захисту. Для того, щоб перевірити систему на слабі місця, хакери проводять сканування портів, запити DNS, ехо-тестування розкритих за допомогою DNS адрес і т.д. За допомогою цих дій, зловмисники можуть з'ясувати, кому належить той або інший домен і які адреси цьому домену привласнені. За допомогою технології ехо-тестування адрес, розкритих за допомогою DNS, хакери можуть побачити, які хости реально працюють в даній мережі, а засоби сканування портів дозволяють скласти повний список послуг, підтримуваних цими хостами.

ВИСНОВОК

Через постійний розвиток технологій викрадення інформації, кожен день виникають нові більш витончені інструменту взлому комп’ютерних систем, тому дуже важливим фактором для захисту корпоративної мережі є спроможність стратегічного планування безпеки та своєчасного підлаштовування до нових типів взлому системи.

З усього цього можна зробити висновок, що основною проблемою захисту інформації в корпоративній мережі в Україні є відсутність чіткого розуміння загрози від кіберзлочинців, а також відсутність розуміння роботи конкретних типів атак, та засобів її знешкодження. Велику роль також відіграє погана підготовка та перевірка кадрів, які, за допомогою методів соціальної інженерії, можуть буди завербовані злочинцями, або просто через своє нерозуміння ситуації впустити ворожу програму в середину мережі. Також потребує допрацювання закон України про кіберзлочинність, через те, що в ньому для злочинців існує багато законних шляхів уникнути покарання.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Григорьев Ю. А. Компьютеные сети/ Григорьев Ю. А. – Москва : 2016. – 425 с. – (Компьютеные сети)

2. Файловий архів [Електронний ресурс]: [http://www.studfiles.ru]. – Корпоративні мережі. – Київ: 2014. – Режим доступу: http://www.studfiles.ru/preview/5025386/

УДК 004.056.53

БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ В КОНТАКТ-ЦЕНТРАХ

Білоусова Вікторія Русланівна
Науковий керівник: Войцех Сергій Іванович
Державний ВНЗ «Національнальний гірничий університет», http://bit.nmu.org.ua/,
E-mail: torybelan94@gmail.com

У роботі розглянуто шляхи забезпечення захисту персональних даних в контакт-центрах від загрози витоку інформації технічними каналами.

Ключові слова – контакт-центр, персональні дані, технічні канали.

ВСТУП

Контакт-центри обробки викликів набули широкого поширення, шо потребує підвищеної уваги до забезпечення захисту інформації від витоку та несанкціонованого отримання. Недостатня захищеність операторських центрів частково пояснюється прагненням їх власників мінімізувати витрати на обслуговування викликів та суттєвою плинністю операторського персоналу[1].

Call-центр (від англ. Call - дзвінок, виклик) - система ефективного зворотного зв'язку зі споживачем товарів і послуг (замовником) або підтримки, просування різних акцій, соціальних опитувань, голосувань. Є частиною CRM-системи, призначеної для автоматизації стратегій взаємодії з замовниками [2].

СТРУКТУРА КОНТАКТ–ЦЕНТРУ

Структурно організація контакт-центру, базується на багатофункціональному програмно - апаратному комплексі автоматичного відправлення, прийому, а також обробки великої кількості вхідних і вихідних телефонних викликів, обробки матеріалів електронної пошти, SMS-повідомлень і Web- запитів. Структура контакт-центру передбачає роботу з численними телефонними зверненнями клієнтів. Ресурси контакт-центру дозволяють зробити дзвінки великого числа потенційних клієнтів в короткі терміни, що в свою чергу впливає на кількість нових клієнтів і розширення клієнтської бази[3].

Складові контакт-центру:

- Операторська лінія обробки - в тому числі і статистичної - вхідних і вихідних телефонних викликів;
- Програмно-апаратний центр управління вхідними та вихідними викликами;
- Центр обробки повідомлень, що надійшли по будь якому каналу зв'язку (телефон, інтернет) [2].

КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ В КОНТАК–ЦЕНТРАХ ТА СПОСОБИ ЗНЯТТЯ МОВНОЇ ІНФОРМАЦІЇ

В контакт-центрах можливі наступні канали витоку інформації: акустичний, віброакустичний, канали перехоплення мовної інформації із телефонних ліній зв'язку. Несанкціоноване отримання мовної інформації здійснюється за допомогою:

- Радіомікрофонів (заносні, заставні);
- Мережевих систем (передача мережею 220В);
- Портативної звукозаписної апаратури (запис інформації учасниками переговорів);
- Кабельні (дротові) мікрофони (закладені з верхніх помешкань у підвісну стелю);
- Спрямованих мікрофонів (через наявність відкритих вікон, кватирок);
- Лазерні мікрофони (зняття інформації із шибки);

ШЛЯХИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОНТАКТ-ЦЕНТРУ

Мережева безпека контакт-центру: розмежовування прав доступу на апаратному рівні (канали зв'язку, телефонна станція, системи розподілу дзвінків, допоміжні сервери);

Організаційна безпека контакт-центру: забезпечення безпеки на рівні «людського фактору». Її реалізація забезпечується суворим дотриманням вимог політики безпеки персоналом контакт-центру[5].

УНИКНЕННЯ ВИТОКУ ІНФОРМАЦІЇ

Уникнення витоку інформації досягається розмежуванням доступу до додатків, в яких містяться дані замовників(клієнтів). Політика безпеки контакт-центру повинна забезпечувати гарантію конфіденційності інформації, отриманої від користувачів. Інформація, яка використовується при запиті, повинна зберігатися в захищеній інформаційній базі. Необхідна систематична перевірка якості роботи контакт-центру та порядності операторів щодо використання клієнтських баз даних. [6].

ВИСНОВКИ

Інформаційна безпека контакт-центрів вимагає постійно уваги до роботи операторів з персональними даними. Необхідно проводити перевірки приміщень контакт-центрів в котрих циркулює інформація з обмеженим доступом. Рекомендовано впровадження КСЗІ для даного роду діяльності.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1.Загальна інформація Контак-центру [Електронний ресурс]. Режим доступу:

https://ru.wikipedia.org

2.Система ефективного зворотного зв'язку зі споживачем товарів і послуг (замовником) або підтримки, просування різних акцій, соціальних опитувань, голосувань [Електронний ресурс]. Режим доступу: http://www.tadviser.ru

3.Структура и функции колл-центра [Електронний ресурс] Режим доступу: http://cartli.ru/articles/funkcii-call-centra

4.Канали витоку інформації [Електронний ресурс] Режим доступу: http://pidruchniki.com/1512021051313/ekonomika/kanali_vitoku_informatsiyi

5.Що таке контакт-центр. Призначенн та задачі [Електроний ресурс]. Режим доступу: http://www.callcenter24.ru/info/23.shtml

6.ЗАКОН УКРАЇНИ «Про захист персональних даних» (Відомості Верховної Ради України [Електронний ресурс] Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-17

УДК 004.7:004.056

ТАКТИКА ВПРОВАДЖЕННЯ MICROSOFT OFFICE 365 НА ПІДПРИЄМСТВІ

Шовкута Володимир Андрійович
Науковий керівник: Флоров Сергій Володимирович
Державний ВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/,
E-mail: v.shovkuta@gmail.com

У статті розглянуто варіанти впровадження Microsoft Office 365 на підприємстві, його переваги та внутрішні та клієнтські засоби забезпечення безпеки Microsoft Office 365 .

Ключові слова – Microsoft Office, Microsoft Office 365, хмарні обчислення, AES, SSL, TLS, Active Directory.

ВСТУП

Багатьом користувачам, що використовують офісний пакет Microsoft Office, важко уявити чим саме є Microsoft Office 365. Вони вважають, що отримують Word, Excel, PowerPoint і інші додатки у «хмарі» для використання у веб-браузері стаціонарного ПК або смартфону.

Так, Microsoft Office 365 передбачає використання аналогів оффлайн версій офісного пакету у вигляді веб-застосунків, але це лише частина пропонованих компонентів, що створюють комплексні і стратегічні напрями в рамках підприємства. Крім таких функцій, як Exchange Online, SharePoint Online або Skype for Business Online, Microsoft Office 365 передбачає функції безпеки, аналіз даних, роботу над проектами, онлайн-комунікацію, соціальні мережі та багато іншого.

ВАРІАНТИ ВПРОВАДЖЕННЯ MICROSOFT OFFICE 365

Microsoft Office 365 постачається у вигляді підписки на пакети, що направленні на різні цілі та сегменти ринку та слугують для забезпечення різних потреб з різними варіаціями цін.

Серед пропонованих пакетів можна виділити різні варіанти відписок для дому та для бізнесу.

Для домашнього використання доступні варіанти:

- Office 365 Home;
- Office 365 Personal;
- Office Home & Student 2016.

У той же час, для корпоративного сегменту варіанти підписки більш різноманітні:

- Office 365 Business;
- Office 365 Business Essentials;
- Office 365 Business Premium;
- Office 365 ProPlus;
- Office 365 Enterprise.

Розглянемо програмні продукти, що включені у різні варіанти.

Office 365 Personal включає доступ до Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft OneNote, Microsoft Outlook, Microsoft Publisher та Microsoft Access для домашнього/некомерційного використання (PC чи Mac), а також передбачає інсталяцію на одному планшеті (Android, iOS чи Windows RT) або телефоні. Додатково до цього є можливість використовувати 1 TB сховища на OneDrive і 60 хвилин міжнародних дзвінків у Skype.

Office 365 Home є аналогічним Office 365 Personal, за винятком того, що Home-версія передбачає використання пакету на п’яти стаціонарних ПК, планшетах і смартфонах, замість одного у Personal.

Office Home & Student 2016 включає у себе лише Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft OneNote для інсталяції тільки на одному стаціонарному ПК.

Версії Office 365 Home та Office 365 Personal передбачає підписку строком на один рік чи місяць, у той час як Office Home & Student 2016 доступний для одноразового придбання.

Office 365 Business надає повний пакет Microsoft Office для інсталяції на стаціонарному ПК, планшеті та телефоні для кожного користувача.

Office 365 Business Essentials надає доступ до бізнес-пошти, OneDrive для бізнесу, Exchange, SharePoint, Lync і Teams сервісів.

Office 365 Business Premium є комбінацією планів Office 365 Business та Office 365 Business Essentials.

Office 365 ProPlus дублює функціонал Office 365 Business, але додатково включає Skype for Business.

Office 365 Enterprise надає доступ до всіх програм Office, Exchange, SharePoint, Teams і Skype, а також особливі сервіси та підтримку для бізнесу.

Всі версії Microsoft Office 365 для бізнесу є річною підпискою з оплатою за кожного користувача [1].

ПЕРЕВАГИ ПІДПИСКИ НА MICROSOFT OFFICE 365 ДЛЯ ПІДПРИЄМСТВА

Існує ряд переваг для підприємства при підписці на Microsoft Office 365, наприклад:

1. Економія. При використанні Office 365 компанії не потрібно купувати власні сервера та комплектуючі. З'являється можливість заощадити на техніці, електроживленні і оренді приміщень. Є можливість платити лише за ті ліцензії, які фактично використовуються.

2. Спрощення IT-інфраструктури. Перехід на роботу з Office 365 дозволяє відмовитися від самостійного розгортання серверів Exchange, Skype for Business і SharePoint, скоротити навантаження на сервер SQL.

3. Гнучкість. Якщо компанія швидко росте або, навпаки, скорочує штат, стає простіше адаптувати структуру IT-сервісів до роботи, підключати або відключати нових співробітників.

4. Мобільність. Office 365 дозволяє отримати доступ до корпоративних ресурсів практично з будь-якої точки – з власного офісу, з офісів партнерів і клієнтів, з дому та інших місць, з мобільного пристрою або звичного комп'ютера.

5. Актуальність. Використання Office 365 забезпечує роботу з останніми і перевіреними версіями програмного забезпечення.

6. Розподіленість. Інформація зберігається у розподілених дата-центрах по світі. Технологія геореплікації забезпечує постійну доступність даних.

ЗАСОБИ БЕЗПЕКИ OFFICE 365

Office 365 – це служба з підвищеним рівнем безпеки, створена відповідно до принципів життєвого циклу розробки захищених додатків Microsoft.

Для забезпечення безпеки на фізичному і логічному рівнях, а також на рівні даних в службі Office 365 використовуються комплексні заходи захисту на основі рекомендацій, вироблених в процесі експлуатації подібних систем.

До вбудованих засобів безпеки належать:

Цілодобовий нагляд за обладнанням. Дані Office 365 зберігаються в мережі центрів обробки даних (ЦОД), які розміщені в стратегічних точках і знаходяться під управлінням служби Microsoft Global Foundation Services. Це гарантує надання послуг і захист інформації від стихійних лих або несанкціонованого доступу. Контроль фізичного доступу здійснюється за допомогою процедур аутентифікації і використання бейджів і смарт-карт, біометричних сканерів, двофакторної автентифікації, в будівлі присутні співробітники локальної служби безпеки, ведеться постійне відеоспостереження. Центри обробки даних обладнані датчиками руху, системами відеоспостереження та сигналізації.

Ізольовані дані клієнтів. Зберігання та обробка даних кожного клієнта здійснюється окремо за допомогою Active Directory і інших засобів, спеціально розроблених для контролю і забезпечення безпеки багатокористувацьких середовищ. Active Directory ізолює клієнтів, використовуючи зони безпеки. Такий підхід не дозволяє одним клієнтам отримати доступ до даних інших клієнтів або поставити під загрозу безпеку цієї інформації.

Захищена мережа. Мережі центрів обробки даних Office 365 сегментовані і забезпечують фізичний поділ критично важливих внутрішніх серверів і пристроїв зберігання від загальнодоступних інтерфейсів. Засоби безпеки прикордонних маршрутизаторів виявляють спроби вторгнення і ознаки уразливості системи. Підключення клієнтів до Office 365 відбувається по протоколу SSL, що забезпечує безпеку Outlook, Outlook Web App, Exchange ActiveSync, POP3 і IMAP. Підключення шифруються з використанням стандартних протоколів безпеки Transport Layer Security (TLS) і Secure Sockets Layer (SSL). Протоколи TLS/SSL гарантують безпечне підключення клієнтів до сервера, конфіденційність і цілісність даних, що передаються між ПК і ЦОД.

Шифрування даних. Вміст електронного повідомлення зашифровано на диску засобом BitLocker за допомогою алгоритму AES з ключем 128 або 256 біт. Під захистом знаходяться всі диски поштових серверів. Крім того, Office 365 здійснює транспортування і збереження повідомлень типу S/MIME, а також повідомлень, зашифрованих за допомогою інструментів шифрування від сторонніх розробників (наприклад, PGP).

Office 365 поєднує в собі пакет додатків Microsoft Office з хмарними версіями служб: Microsoft Exchange Online, Microsoft SharePoint Online і Microsoft Lync Online. Кожна служба має власні функції безпеки, якими може керувати клієнт.

Керування функціями безпеки передбачає:

Використання функцій шифрування. Увімкнувши служби шифрування Office 365, з'являється можливість шифрувати переписку з сторонніми користувачами. Адміністратори можуть задавати алгоритми шифрування і підписування документів.

Надання доступу користувачам. Послуги Office 365 захищаються на наступних рівнях: ЦОД, мережевий, логічний, рівень зберігання та передачі. Office 365 інтегрується з локальної службою каталогів Active Directory і іншими системами зберігання і ідентифікації каталогів.

Двофакторна перевірка автентичності. Двофакторна перевірка автентичності підвищує рівень безпеки в середовищі з безліччю пристроїв, орієнтованої на хмарні технології. Компанія Microsoft пропонує рішення для двофакторної перевірки автентичності з можливістю аутентифікації за телефоном, а також підтримує рішення сторонніх розробників. При двофакторній перевірці автентичності з використанням телефону користувач

отримує СМС повідомлення з кодом і вводить його в якості другого пароля при вході в службу [2].

ВИСНОВОК

Щороку з'являються нові версії програмного забезпечення, що розширюють вже існуючий функціонал. У разі ігнорування IT-відділом цих оновлень, залишаються помилки у встановлених програмних продуктах та недоступні функції нових версій продукту. Використання Office 365 дозволяє компаніям використовувати останні версії програмного забезпечення Microsoft.

Впровадження Office 365 забезпечує стійке шифрування як для даних, що передаються між кліентом і ЦОД, так і при зберіганні у ЦОД. Розподіленість ЦОД та реплікація гарантує доступність даних в незалежності від стихійних лих чи інших факторів, а гнучкі налаштування доступу для користувачів, забезпечують необхідний захист від інсайдерів та несанкціонованого доступу.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Get the most from Office with Office 365 [Електронний ресурс]. – Режим доступу: https://products.office.com/en-us/compare-all-microsoft-office-products (дата звернення 05.04.2017), вільний.

2. Средства безопасности Office 365 [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/ru-RU/download/confirmation.aspx?id=26552 (дата звернення 05.04.2016), вільний.

УДК 004.056

АНАЛІЗ ПОБУДОВИ БЛОКІРАТОРІВ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ З ІНТЕЛЕКТУАЛЬНИМ БЛОКУВАННЯМ

Потоцький Сергій Вікторович

Науковий керівник: Войцех Сергій Іванович

ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/, E-mail:s90992p@yandex.ua

Проаналізовані діючі стандарти мобільного зв'язку в Україні, переваги та недоліки побудови блокіраторів стільникового зв'язку з різними режимами роботи. Основну увагу приділено особливостям структурної побудови блокіраторів з інтелектуальним режимом блокування.

Ключові слова – стільниковий зв'язок, стільниковий телефон, блокіратор, синтезатор, модулятор, передача даних.

На сьогодні в Україні діють наступні стандарти мобільного зв'язку: GSM, GPRS, EDGE, CDMA2000, UMTS.

GSM (Global System for Mobile Communications) – міжнародний стандарт цифрового стільникового зв'язку з часовим розподілом каналів (TDMA) та відносно високим рівнем безпеки за рахунок застосування шифруванню з відкритим ключем. В Україні використовується частотні діапазони 900 МГц та 1800 МГц.

GPRS (General Packet Radio Service) – пакетний радіозв'язок загального користування – (надбудова над технологією мобільного зв'язку GSM), що здійснює пакетну передачу даних. GPRS дозволяє користувачеві мобільного телефону (МТ) проводити обмін даними з іншими пристроями в мережі GSM і з зовнішніми мережами, в тому числі Інтернет. GPRS. Теоретично швидкість передачі досягає до 100 кбіт/с.

EDGE (Enhanced Data rates for GSM Evolution) – цифрова технологія для стільникового зв'язку, яка функціонує як надбудова над GPRS мережами. Ця технологія працює в TDMA і GSM мережах. швидкість передачі теоретично досягає до 474 кбіт/с.

CDMA2000 - стандарт зв'язку третього покоління. У CDMA використовується кодове розділення сигналів. Кожен абонент, підключений до базової станції (БС), використовує весь доступний частотний ресурс, загальний для всіх абонентів, а базова станція спілкується з усіма одночасно. Сигнал від конкретного користувача виділяється за допомогою кодової модуляції – кожному абоненту відповідає специфічний «код», що дозволяє виділити його із загального радіоефіру. На сьогодні є три модифікації. 1X EV-DO Rev. 0, швидкість передачі — до 2,4 Мбіт/с, 1XEV-DO Rev A, передача даних зі швидкістю до 3,1 Мбіт/с. 1XEV-DO Rev B, з метою досягти наступних швидкостей на одному частотному каналі: 4,9 Мбіт/с до абонента і 1,8 Мбіт/с від абонента.

UMTS (англ. Universal Mobile Telecommunications System — Універсальна Мобільна Телекомунікаційна Система) — технологія стільникового зв'язку для впровадження 3G в Європі. В якості способу передачі даних через повітряний простір використовується технологія W-CDMA. UMTS (або W-CDMA) (Wideband Code Division Multiple Access), оптимізована для надання високошвидкісних мультимедійних послуг, доступу в Інтернет і відеоконференцій. Ширина смуги W-CDMA становить 5 МГц. На даний час використовуються технології передачі даних HSPA, що дозволяє отримати швидкість передачі до 14,4 Мбіт/с.

Класифікація різновидів блокіраторів наведена у [3].

Однією із основних характеристик блокіраторів є радіус дії, який залежить від вихідної потужності підсилювача генератора завад, а також від відстані виділеного приміщення (ВП) до БС. Для блокіраторів з ручним керуванням вихідна потужність кожного

генератора варіюється від 0,5 Вт до 2 Вт для портативних блокіраторів і від 8 Вт до 10Вт для стаціонарних. Ефективний радіус придушення для стаціонарних блокіраторів 3-50м, для портативних -3-10м. Основним недоліком блокіраторів з ручним керуванням є безперервність випромінювання, що може негативно впливати на здоров'я користувачів та обмежує час роботи від акумуляторної батареї. Широкий спектр випромінюваного сигналу може приводити до збоїв у роботі технічних засобів обробки інформації та допоміжних технічних засобів і систем. Необхідність охолодження вихідних каскадів генераторів призводить до збільшення габаритних розмірів пристроїв.

Режим інтелектуального блокування орієнтований на конкретний стандарт зв'язку, конкретний канал, на момент запиту чи встановлення зв'язку. Структурна схема представлена на рисунку 1. Сигнал з ефіру поступає на приймальну антенну W1 і далі на вхід панорамного приймача, який сканує у реальному масштабі часу діапазон частот у направлені МТ - БС відповідного стандарту зв'язку. Сигнал з приймача поступає цифровий блок обробки сигналів, де відбувається аналіз небезпечного сигналу та декодування. Процесом сканування та обробки сигналу керує контролер. На основі аналізу і декодування прийнятого сигнал, контролер відповідно до певного алгоритму формує сигнали

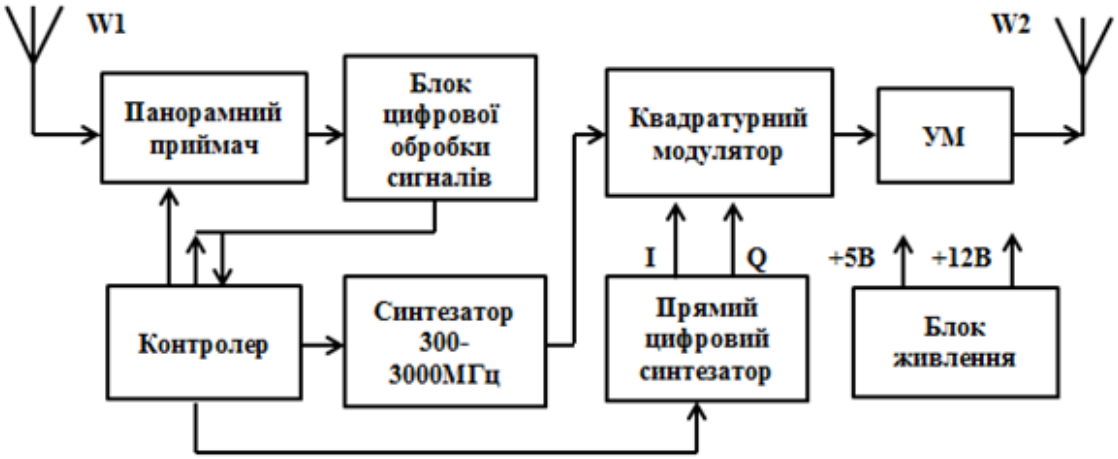


Рисунок.1 Структурна схема системи інтелектуального блокування.

упраавління синтезатором високочастотного сигналу та прямим цифровим синтезатором. Високочастотний широкосмуговий синтезатор виробляє сигнал у широкому діапазоні частот (300-3000МГц) , що далі надходить на квадратурний модулятор. Прямий цифровий синтезатор формує квадратурні складові (I,Q) модулюючого сигналу, що дозволяє одержати на виході модулятора сигнали з різними видами модуляції. Смуга сигналу може варіюватися в межах від 0 до 200 МГц. Сигнал з модулятора надходить на широкосмуговий підсилювач потужності і на антену W2. Для зменшення рівня побічних складових може застосовуватися система діапазонних фільтрів.

ВИСНОВОК

Переваги систем інтелектуального блокування поширюють перспективи їх подальшого застосування. При реалізації таких систем найважливішим завданням є реалізація алгоритму виявлення, декодування небезпечного сигналу для генерації сигналу придушення. Розвиток стандартів стільникового зв'язку вимагає постійної уваги до створення нових алгоритмів виявлення небезпечного сигналу та генерації сигналу придушення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стандарты сотовой связи [Електронний ресурс]. Режим доступу - [http://zvyazok.com.ua/articles/standartyi-sotovoy-svyazi].

2. Блокираторы сотовой телефонии [Електронний ресурс]. Режим доступу - [http://www.radioservice.ru/public/catalog.pdf].

3. Защита акустической речевой информации с ограниченным доступом от утечки по техническому каналу при использовании средств мобильной связи: матеріали VIII Всеукр. наук.-практ. конф. (м. Дніпро 24 лист. 2016) ДВНЗ «Національний гірничий університет» С.В.Потоцький, 2016.-21 с.

UDC 004

INVESTIGATION OF USING QUANTUM COMPUTERS POSSIBILITY IN CRYPTOGRAPHY

Masalskaya O., Mieshkov V.
National mining university
http://bit.nmu.org.ua

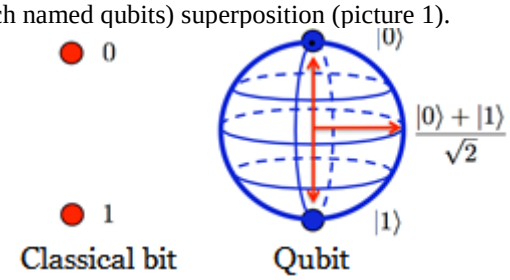
Introduction

Internet purchases and payments by credit card require the encrypted data transfer using special parameter called a key. Today the most common methods based on public-key cryptography are, for instance, RSA algorithm, El-Gamal algorithm or elliptic curve's cryptosystem. It is very difficult to crack such cryptosystems but it is theoretically possible and the quantum computers development, so widespread now, is a reliable way to do this. It will be possible because of huge increase of quantum computations velocity compare to traditional computing.

Encryption is a kind of information transformation, which makes it accessible only to legitimate users (for example, for the buyer and the store server). The principle of cryptography with a public key is based on the fact that the parties of exchanging information for the development of the key carry out a series of calculations. It's important to note that the calculation's process not requires the complete set of input data exchange. The confidentiality of the key generated by this way is guaranteed by the fact of having only the data transferred in the calculations, the attacker will spend a lot of time searching for the key (it is considered that he solves the "computationally complex problem", that is, the problem for which the effective polynomial algorithm is unknown). And it means cryptosystems on public keys are hacking using the existing computing resources for a time longer than the time of Universe existence [1].

Quantum computers

A quantum computer differs from the classical one in that it's structural elements are not the usual transistors but quantum objects are photons or atoms. Obeying the laws of quantum mechanics, these objects are in a state of superposition. Thus, if the quantum system has two admissible states (conditionally, "1" and "0"), then up to the measurement moment is in their (photons or atoms which named qubits) superposition (picture 1).



Pic. 1 - Qubit superposition

This gives a certain gain in various calculations. Examples of such problems as was shown by the American mathematician Peter Shore are the problems of factorization and discrete logarithm finding. It is because of the complexity of these tasks for modern computers that it is possible to use them (computers) for cryptographic systems with public key. In addition, there is no mathematical proof of the absence of a classical (non-quantum) algorithm for solving factorization and discrete logarithm problems, since there is no single algorithm for reducing the problem from the NP-class to a series of P class problems, which can be efficiently computed. A full-fledged quantum computer can easily cope with similar problems [2].

Public Key Cryptography Alternatives

In the information space cryptography is one of the main tools and information security is one of the main existence conditions. Let's consider alternatives to asymmetric cryptography. The first alternative is to come up with a task that would be difficult for a quantum computer. Such problems are exist, they are learned by post-quantum cryptography. However nobody guarantees that there is no classical or quantum algorithm that can solve this problem quickly. Therefore, such systems will always be under threat.

Physicist Charles Bennett and mathematician Gilles Brassard proposed another elegant way out of this situation. Shore's work shows that quantum technologies can become a destructive force for modern information infrastructure, whereas Bennett and Brassard's work (written 12 years earlier than Shor's article in 1984) reveals the enormous potential of quantum physics for the new cryptographic systems creation.

The physical principles of quantum cryptography (or, more accurately, of quantum key distribution) are quite simple. If quantum objects were used as data carriers then appears opportunity to find out if there was an interception attempt. In this case, the quantum nature of information carriers limits the potential of the potential violator: when someone try to intervene in the transmission process, it introduces noise that can always be recorded. Thus, in reality, quantum is the key transfer itself but all other processes are classical.

Bennett and Brassard proposed a practical recipe, called the BB84 protocol, for quantum key distribution: it was supposed to use photons in orthogonal polarization bases [3]. BB84 is the first quantum cryptography protocol. The protocol is provably secure, relying on the quantum property that information gain is only possible

at the expense of disturbing the signal if the two states one is trying to distinguish are not orthogonal.

However, for an industrial system of quantum cryptography, it is not enough to exchange photons. In quantum keys errors are always exist, which are caused by technical imperfection of the equipment. Such errors must be corrected, otherwise it cannot be used for encryption. The model of secrecy of quantum cryptography is "excessively protected" because all errors introduced during transmission (even if they are known as of the attenuation of an optical signal in a fiber-optic cable) are considered to be caused by the actions of the attacker. Then need to evaluate whether the attacker could recover the key from the available information. During the error correction, procedure a certain amount of information is inevitably disclosed, so at the final stage it is necessary to clean out the potentially known information about the key using a procedure called secrecy. Finally, all messages on the auxiliary (classical) channel should not be distorted. Thus, industrial quantum cryptography does not finish with photon transfer technology, but forms a sphere at the intersection of physics, information theory and engineering.

Quantum key distribution works rather slowly, so using the quantum keys for encryption with one-time notebooks makes sense for very important and valuable information. For practical durability, it is possible to build hybrid systems. In such systems, a quantum key is used on a par with classical keys "wired" into telecommunications equipment. Such solutions allow, at first, to increase the security of systems. Secondly, they allow the quantum key distribution to seamlessly integrate into the existing information and telecommunications infrastructure [4].

The processing of quantum cryptography without the use of cables is one of the scientific tasks for China's recently launched satellite. Such experiments are the basis for global systems of future information protection, based on quantum communications.

Conclusions

Thus, quantum technologies change our understanding of the security of information, providing us with a new and powerful computing weapon - a quantum computer. In addition, quantum physics provides us with a method that ensures the information protection at the level of fundamental laws. However, to preserve the familiar forms of information exchange, steps are required to introduce quantum cryptography.

1. Сушко С.А. и др. Криптография. НГУ. Днепропетровск.

2. Против паранойи: квантовый компьютер как угроза информационной безопасности. [Електронний ресурс]: http://ai-news.ru/2016/09/protiv_paranoji_kvantovyj_komputer_kak_nbsp_ugroza_informacionnoj_bezopasno_643775.html

3. Протокол квантового распределения ключа [Електронний ресурс]: https://ru.wikipedia.org/wiki/BB84

4. Quantum cryptography [Електронний ресурс]: https://en.wikipedia.org/wiki/Quantum_cryptography

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

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ. БЕЗПЕКА ТА ЗВ'ЯЗОК

20 квітня 2017 р.

Підписано до друку 20.04.17. Формат 30 х 42/2.
Елект. видання.

Підготовлено до друку у Державному ВНЗ
«Національний гірничий університет»
49005, м. Дніпро, просп. Д. Яворницького, 19