Список використаної літератури. ***1.*** *Ленков С. В. Методы и средства защиты информации. В 2-х томах /Ленков С. В., Перегудов Д. А., Хорошко В. А.– К.: Арий,2008.* ***2.*** *Емельянов С. Л. Проблемы защиты информации от утечки и пути ее решения / Емельянов С. Л.– Одесса: Фенікс, 2011. – с. 624* ***3.*** *Артемов В. Ю. Нормативно-правовий довідник з охорони інформації в Україні. У 4-х томах / Артемов В. Ю., Лєнков О. С., Пашков А. С., Стаднік О. М., Хорошко В. О. – К.: Вид. ДУІКТ, 2010.* ***4.*** *Бабак В. П. Теоретические основы защиты информации / Бабак В. П., Ключников А. А. – НАН Украины, Ин-т проблем безопасности АЭС.– Чернобыль (Киев.обл.): Ин-т проблем безопасности АЭС, 2012.– с.776* ***5.*** *Хорошко В. О. Методичне забезпечення підготовки та перепідготовки спеціалістів з інформаційної безпеки / Хорошко В. О., Орєхова І. І. // Сучасна спеціальна техніка, №3, 2011. – С. 22-27.*

Дмитро Мехед
Чернігівський національний технологічний університет

УДК 004.773

ІНФОРМАЦІЙНА БЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ. МЕТОДИ ПОШИРЕННЯ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Анотація: **Розглядаються соціальні мережі, основні методи поширення інформації в соціальних мережах, зроблено аналіз переваг і недоліків різних методів захисту інформації. Проаналізовано метод визначення стратегії розповсюдження інформації в соціальній мережі, виділено основні параметри, які є базовими для забезпечення захисту інформації, можливість втрати інформації, а також методи її захисту.**
Summary: **In the article the social networks, the main methods of dissemination of information in social networks, the analysis of the advantages and disadvantages of various methods of data protection. The analysis method for determining the strategy of information dissemination in social networks highlights the main parameters that are fundamental to protect information, the possibility of loss of information, as well as methods of protection.**
Ключові слова: **Інформація, інформаційна безпека, соціальні мережі.**

Характерною особливістю сучасності є та обставина, що до активної участі в інформаційних процесах у дуже стислі строки долучилися широкі маси користувачів, що в переважній більшості не мають відповідного рівня підготовки до участі в суспільно корисній інформаційній діяльності. Для значної частини учасників інформаційних обмінів самовираження в Інтернеті поки що є значущим як процес. І тому сьогодні інформаційний простір перевантажений випадковою, низькоякісною інформацією, що ускладнює використання суспільно значущих ресурсів. Однак останнім часом з розвитком інформаційних технологій, удосконаленням загальносуспільної системи соціальних інформаційних комунікацій в Україні ми спостерігаємо характерний також і для інших країн світу процес самоорганізації вітчизняного інформаційного простору, формування системи соціальних інформаційних мереж [1].

Є два різні способи, за допомогою яких людина отримує інформацію в мережі: – через зв'язки в соціальних мережах і під впливом зовнішніх немережевих джерел, таких як традиційні ЗМІ [2]. Хоча більшість нинішніх моделей сприйняття інформації в мережах виходять з того, що інформація лише передається від одного вузла до іншого по краях (периферії) базової мережі, доступність даних в масових соціальних мережах в Інтернеті дозволяє нам докладніше дослідити цей процес. Таким чином соціальні мережі відіграють фундаментальну роль у поширенні інформації.

Соціальна мережа (від англ. Social networking service) – платформа, онлайн сервіс або веб-сайт, призначені для побудови, відображення та організації соціальних взаємовідносин, візуалізацією яких є соціальні графи [3]. Наразі кількість соціальних мереж в Інтернеті і число їх користувачів швидко зростає (соціальні мережі стартували в 1995 р, в 2000-і набули глобального розмаху).

Соціальні мережі – явище нове, але йому передував ряд філософських концепцій. Наприклад, китайська концепція Guanxi про використання особистого впливу на основі особливого виду особистих відносин, таких як повага, дружнє ставлення та готовність надати один одному взаємну допомогу або послугу [3]. Цю концепцію пов'язують з поняттями «суспільство», в якому індивіди більш орієнтовані на дотримання інтересів оточуючих, ніж своїх власних.

Особиста інформація ще ніколи не була такою доступною, як нині. Ситуація загострюється ще й через те, що більшість користувачів не знає елементарних правил безпеки онлайнового спілкування і використання

соціальних мереж. Більшість людей намагаються перетворити на реальність слова: «все, що ви скажете в соціальних мережах, може бути використано проти вас». В сучасному суспільстві є звичка використовувати соціальні мережі й інтернет, але практично не вироблена культура онлайн-спілкування і використання соціальних сервісів [4].

Аналіз останніх досліджень і публікацій. Дослідженню питань інформаційної безпеки присвячені роботи В. М. Богуна, С. В. Віхорева, І. Д. Горбенко, Ю. І. Грицюк, М. А. Жалдака, С. В. Казмирчук, Г. Ф. Конаховича, О. Г. Корченка, М. Г. Луцького, А. І. Марущака, В. П. Мельнікова, В. В. Мохора, О. М. Новікова, О. В. Олійника, С. А. Ракова, О. В. Сосніна, С. В. Толюпи, В. О. Хорошко, О. К. Юдіна та ін.

Виділення не вирішених раніше частин загальної проблеми. Незважаючи на значний обсяг накопичених у даній сфері знань, недостатньо дослідженою залишилась проблема захисту інформації соціальних мереж.

Метою дослідження було охарактеризувати та систематизувати методи поширення інформації в соціальних мережах, висвітлити основні причини можливості втрати інформації та методи її захисту.

Виклад основного матеріалу. Поняття «соціальні мережі» вперше ввів соціолог Джеймс Барнс: «Соціальна мережа (Social Network) – це соціальна структура, що складається з групи вузлів, якими є соціальні об'єкти (люди або організації), і зв'язків між ними» [5].

У найпростішій формі соціальна мережа - це карта всіх релевантних зв'язків між вузлами. Формально соціальна мережа являє собою граф S (G, E), в якому G = {1, 2, ..., n} - множина вершин (агентів) і E - безліч ребер, що відображають взаємодію агентів. Агент - це вузол соціальної мережі (вершина графа). Агентами можуть стати різні субагенти, наприклад сім'ї, групи, організації. Зв'язки між агентами - це відносини, наприклад, знайомство, дружба, співпраця, комунікації. Агенти залежно від інформації, якою вони володіють, можуть впливати на прийняття рішення, на інших агентів, інформаційне управління та інформаційне протиборство.

Якщо розглядати соціальну мережу більш глибоко, можна виявити, що зв'язки діляться за типами: односторонні і двосторонні; мережі друзів, знайомих, колег, однокласників, однокурсників, однодумців і т. д. Соціальна мережа – це ще й засіб спілкування. Будь-якій людині емоційно важлива думка інших людей, в тому числі, коли все добре – їх визнання, а коли наступила смуга невдач – співчуття і співучасть. Ритм життя стає таким, що часу на традиційне спілкування з друзями зараз залишається все менше і менше. І соціальні мережі з цієї точки зору – незамінна річ, оскільки дають можливість спілкуватися, не витрачаючи часу на дорогу, не погоджуючи зручні проміжки часу.

Одним з результатів взаємодії людей за допомогою таких мереж є отримання величезної кількості інформації різних форматів: тексти, картинки, аудіо, відео та ін. Сьогодні соціальні мережі надають користувачам широкий функціонал для обміну інформацією, їх відвідує більш ніж дві третини онлайн-аудиторії у всьому світі, і це четверта за популярністю онлайн-категорія після пошукових і інформаційних порталів та програмного забезпечення.

Розглянемо методи поширення інформації в соціальних мережах.

Контекстна реклама. Даний метод поширення інформації в соціальній мережі дозволяє демонструвати рекламні оголошення на особистій сторінці користувача і в додатках соціальної мережі згідно з обраними параметрами. Основною перевагою даного методу є можливість вибору цільової аудиторії по ряду параметрів: демографія, географія, інтереси, освіта, робота та інші параметри. Даний вид поширення інформації є платним, але має високу ефективність. Інформація, поширювана через контекстну рекламу, має обмеження, встановлені адміністрацією соціальної мережі. Вся поширювана інформація проходить модерацію перед розповсюдженням. Протизаконна інформація не може бути поширена через контекстну рекламу.

Масова розсилка особистих повідомлень (спам). Даний вид поширення інформації в соціальній мережі передбачає розсилку особистих повідомлень користувачам. Розсилка спаму є безкоштовним засобом доставки контенту користувачам, але адміністрація соціальної мережі бореться з цим явищем. Для обмеження розсилки спаму адміністратори блокують акаунти, обмежують кількість відправлених повідомлень, вимагають прив'язки аккаунта до телефону, обмежують обсяг вибірки за запитом, встановлюють спам-фільтри, дають можливість вносити користувачів в чорні списки і позначати повідомлення як спам для виключення подальшого їх отримання. Даний метод поширення інформації є частково неконтрольованим; користувач може поширювати будь-яку інформацію, у тому числі протизаконну.

Несанкціонована розсилка повідомлень по «стінам» великих спільнот. Даний метод поширення інформації в соціальних мережах є більш ефективним, ніж розсилка особистих повідомлень. Даний метод дозволяє охопити більшу аудиторію, також не схильний модерації з боку адміністрації соціальної мережі. Захистом спільноти від нелегітимної інформації в даному випадку займаються адміністратори спільноти.

Розміщення інформації у власному співтоваристві або тематичному обліковому записі. Даний метод поширення інформації в соціальній мережі є найпопулярнішим серед безкоштовних методів. Для охоплення необхідної аудиторії співтовариство спочатку має набрати необхідну масу учасників. З ростом популярності спільноти підвищується його пошуковий індекс в соціальній мережі, що в свою чергу дозволяє залучати більшу кількість користувачів. Важливою перевагою даного методу є високий ступінь довіри користувачів до інформації, що публікується.

Конкурси в соціальній мережі. Даний метод є наймолодшим і передбачає проведення промо-конкурсів для залучення користувачів. Для участі в даному конкурсі користувач повинен поділитися інформацією зі своїми друзями, у відсилаємому повідомленні якраз міститься поширювана інформація і запрошення взяти участь у конкурсі. Перевагою даного методу поширення інформації є висока швидкість розповсюдження і довіра до інформації з боку користувачів.

Розглянуті вище методи поширення інформації є ефективними інструментами для охоплення онлайн-аудиторії. Кожен метод має свої переваги і недоліки. Важливою з точки зору ініціатора поширення інформації є задача вибору методів поширення з мінімальними затратами ресурсів. Для вирішення даної задачі розробимо метод визначення стратегії розповсюдження інформації в соціальній мережі.

На підставі наведених значень характеристик методів можна розробити метод визначення стратегії розповсюдження інформації в соціальній мережі. Метод включає наступні елементи:

1) визначення характеристик рекламного проекту;

2) визначення переліку застосовних методів поширення інформації;

3) визначення можливостей одночасного застосування доступних методів, або окремих найбільш ефективних в даних умовах методів;

4) оцінка охоплення аудиторії поширення інформації.

Будучи однією зі складових інформаційної безпеки суспільства культурна безпека впливає на інші складові національної стабільності та благополуччя. У соціальних мережах міститься велика кількість особистої інформації про учасників, наприклад, інтереси, друзі, демографія та ін. Це може призвести до несанкціонованого поширення особистої інформації в мережах. У рішенні такого типу завдань корисно застосовувати моделі на основі механізмів конфіденційності.

Учасники соціальної мережі, щоб вона існувала, повинні ділитися один з одним певною частиною своєї особистої інформації. В останні 3 – 4 роки тема інформаційної безпеки та приватності в соціальних мережах привертає багато уваги. Це цілком зрозуміло: мережі все більше відкриваються зовнішньому світу, були випадки витоку особистих даних, аккаунти користувачів легко зламуються, а в адміністрації мереж є доступ до будь-якої інформації. Але все це тільки зовнішня частина, яка лежить на поверхні і про яку пише преса, проте далеко не повна картина потенційних загроз для особистих даних. Із психологічної точки зору Інтернет сприймається людиною на рівні натовпу. А в натовпі, як відомо, обличчя і індивідуальність зникає, а з нею і відповідальність [6].

Самим нешкідливим, на перший погляд, варіантом використання особистих даних без дозволу користувача можна вважати внутрішні механізми соціальних мереж для показу реклами, підбору потенційних знайомих або відбору потенційно цікавого контенту. Ці механізми стали стандартом майже у всіх соціальних мережах, і ніхто не приховує даний факт: всі вони збирають і аналізують особисті дані, яких у будь-якій мережі дуже багато, а потім використовують їх у комерційних цілях. Більше того, соціальні мережі передають особисті дані у зовнішній світ, і вже офіційно встигли визнати цей факт.

Більше проблем користувачам створює витік особистих даних з вини мережі, що неодноразово траплялося в різних проектах. Однією з найбільших за розмірами можна вважати витік особистих даних 77 млн. користувачів ігрової мережі PlayStation Network у квітні 2011 року, і ще до кінця не ясні наслідки цього інциденту. Як правило, у подібних випадках має місце витік платіжних даних користувачів.

Ще більш серйозні проблеми може викликати злом окремих аккаунтів і отримання доступу до всієї особистої інформації окремого користувача, якщо мета зловмисників – певна людина. Зробити сьогодні це не складно навіть для буденного користувача, який просто знає людину і може використовувати соціальну інженерію, а крім того є спеціальні послуги по злому, вартість цього всього 20 $. Мотивація зловмисників може бути різноманітною, від злому аккаунтів посадових осіб певної компанії з метою промислового шпигунства до особистих цілей. Так, наприклад, шлюбні юристи США вже зараз фіксують кожен п'ятий випадок розлучення через соціальні мережі: подружжя отримують доступ до профілю партнера, знаходять там переписку з коханцем / коханкою, і в результаті це призводить до розлучення [7].

Окремо варто згадати про віруси і фішинг, які можуть непомітно для користувача красти логіни і паролі і після використовувати їх для незаконних дій (наприклад, автоматична розсилка спаму від імені користувача).

Однак найбільша загроза полягає в тому, що доступ до всієї особистої інформації є у досить великої групи людей, і вони можуть в будь-який момент її переглядати, навіть, якщо людина видалила щось з

мережі. По-перше, це співробітники самої соціальної мережі: у них є доступ до баз даних, в яких міститься вся інформація, а також спеціальні інструменти входу в аккаунти користувачів, як, наприклад, спеціальний майстер-пароль в Facebook, який дозволяє увійти в будь-який аккаунт. По-друге, доступ до інформації також мають правоохоронні органи, такі як ЦРУ в США або ФСБ в Росії.

Останнім часом користувачі все менше довіряють соціальним мережам і все частіше починають фільтрувати інформацію, яку готові довірити мережі, давати неправдиву інформацію або взагалі видаляються з мережі, однак навіть видалення не дає впевненості: часто інформація зберігається на серверах компанії і може використовуватися в подальшому. Зокрема так робить Facebook, ВКонтакте і інші мережі.

Виділимо основні параметри, які є базовими для забезпечення захисту інформації:

- конфіденційність - гарантія того, що конкретна інформація доступна тільки тому колу осіб, для кого вона призначена; порушення цієї категорії називається розкраданням або розкриттям інформації;
- цілісність - гарантія того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;
- автентичність - гарантія того, що джерелом інформації є саме та особа, яку заявлено як її автора; порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення;
- апелюємість - гарантія того, що при необхідності можна буде довести, що автором повідомлення є саме заявлена людина, і не може бути ніхто інший; відмінність цієї категорії від попередньої в тому, що при підміні автора, інша людина намагається привласнити собі авторство повідомлення, а при порушенні апеллюємості – сам автор намагається «відхреститися» від своїх слів.

Загрози інформаційної безпеки – це зворотний бік використання інформаційних технологій. Загроза – це потенційна можливість певним чином порушити інформаційну безпеку.

При системному розгляді різних видів порушень захисту конфіденційної інформації в соціальній мережі відповідно до якісно-кількісних характеристик циркулюючої всередині мережі інформації необхідними для оцінки її вразливостей за ступенем важливості для механізмів захисту можна виділити наступні типи основних загроз інформації в соціальній мережі:

- загроза конфіденційності (витік конфіденційної інформації та заподіяння прямого або непрямого збитку користувачеві соціальної мережі);
- загроза цілісності (модифікація інформації усередині мережі інформації і втрата її адекватності);
- загроза доступності (порушення доступу до мережевої інформації і блокування доступу до ресурсу);
- загроза повноті (знищення інформації усередині мережі та заподіяння прямого або непрямого збитку як користувачеві соціальної мережі, так і її власнику);
- загроза актуальності (затримка отримання легальним користувачем мережі інформації);
- загроза важливості (несанкціоноване читання конфіденційної мережевої інформації, що призводить до втрати її ціннісних характеристик);
- загроза адресності (переадресація мережевої інформації, що може призводити до зниження її конфіденційності та доступності);
- загроза надмірності інформації (багаторазове дублювання мережевої інформації).

На жаль, на законодавчому рівні проблема щодо захисту інформації користувача недостатньо опрацьована. Забезпечення безпеки персональних даних в більшості випадків регламентується виключно правилами захисту інформації про користувачів і правилами користування сайтом.

Висновки. Розвиток електронних технологій дозволяє мільйонам людей вільно користуватись мережею, що дає змогу використовувати їх творчий потенціал для вирішення інтелектуальних, наукових, суспільно значимих питань. В силу причин, описаних у даній статті, можна зробити висновок, що тема захисту інформації користувачів в соціальних мережах залишатиметься актуальною як мінімум в найближчі роки. Проблеми захисту інформації в даній сфері досі остаточно не вирішені і можуть вирішитися тільки в результаті комплексного підходу, що включає в себе спільну роботу творців і розробників мережі, користувачів і держави. Особливого значення набуває питання захисту інформації на фоні формування горизонтальних, корпоративних зв'язків з використанням електронних технологій, зокрема у сфері освіти, а також серед наукової спільноти.

Список використаної літератури. ***1.*** *Соціальні мережі як чинник розвитку громадянського суспільства : [монографія] / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.] ; НАН України, Нац. б-ка України ім. В. І. Вернадського. – К., 2013. – 220 с.* **2.** *Типове положення про службу захисту інформації в автоматизованій системі. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=39738&cat_id=38.* ***3.*** *Соціальна мережа (Інтернет) . – Режим доступу: https://uk.wikipedia.org/wiki/Соціальна_мережа_(інтернет)* ***4.*** *Баловсяк Н. Соціальні мережі вбивають приватність / Тиждень.ua., 2013/ - Режим доступу: http://tyzhden.ua/Society/70950.* ***5.*** *Barnes J. A. Class and Committees in a Norwegian*

Island Parish // Human Relations. 1954. №7. Pp. 39-58. ***6.*** *Соціальні мережі – реальні загрози віртуального світу. – Режим доступу: http://ogo.ua/articles/view/2011-02-23/26490.html.* ***7.*** *Как социальные сети разрушают брак. – Режим доступу: http://letidor.ru/article/kak_sotsialnye_seti_razrushayu_138521/*

Владимир Бурячок, Андрей Орехов, Владимир Хорошко
Национальный Авиационный Университет

УДК 004.621.5

ОПТИМИЗАЦИЯ АРХИТЕКТУРЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА СУВД

Аннотация: ***Приведена методика формирования профиля защищенности, которая позволяет осуществить выбор оптимального варианта построения системы комплексной защиты информации для информационного пространства системы управления воздушным движением (СУВД).***

Annotation: ***The article describes the method of forming the profile of security, which allows for selection of the optimal variant of building a system of complex information protection to the information space air traffic control system.***

Ключевые слова: ***система защиты информации, информационное пространство, система управления воздушным движением, профиль защищенности, архитектура.***

I Введение

Важным является вопрос оптимизации и унификации подходов к реализации мероприятий по обеспечению информационной безопасности как наиболее сложному и трудоемкому компоненту, обеспечивающему безопасность информации в системе управления воздушным движением. Особую роль играет при этом правильный выбор архитектуры системы защиты.

Целью защиты информации в СУВД является деятельность, направленная на предотвращение утечки ее по различным каналам и их блокирования.

Основной стратегией защиты информации является выбор основных и наиболее важных базовых системно-концептуальных положений и ориентиров при планировании, разработке и реализации этой стратегии. Основы стратегии защиты информации включают в себя необходимость использования двух терминологических понятий [1, 2]:

- стратегия технической защиты информации;
- стратегия безопасности защищаемой информации.

На практике в большинстве случаев системы защиты состоят из нескольких звеньев и рубежей. При попытке преодолеть защиту злоумышленник пытается использовать наиболее слабое направление или рубеж в этой системе. По этой причине итоговая прочность системы комплексной защиты информации (СКЗИ) будет определяться прочностью наиболее слабого направления или рубежа в этой системе.

II Основная часть

Так как итоговая прочность СКЗИ определяется прочностью наиболее слабого звена, рубежа или направления в этой системе, то, следовательно, если прочность слабого звена, рубежа или направления не удовлетворяет заданным и требуемым уровням, то это звено, рубеж или направление укрепляется или заменяется на более прочный.

Исходя из этого вероятность эффективной защиты информации при многорубежной системе определяется зависимостью:

$$P_{ИТ} = P_{СКЗИ_1} \cdot P_{СКЗИ_2} \cdot \ldots \cdot P_{СКЗИ_N},$$

где $P_{СКЗИ_N}$ - вероятность эффективной защиты *n*-го рубежа СКЗИ, *n* – порядковый номер рубежа.

Под задачей синтеза комплексной системы защиты информации понимается этап формирования профиля защищенности информационного пространства (ИП) как основополагающий при создании СКЗИ. В общем виде задача синтеза сводится к формированию оптимального варианта реализации профиля защищенности, обеспечивающего максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на создание СКЗИ информационного пространства СУВД. В соответствии со стандартом [3], известным также как "Общие критерии, разработка профиля защищенности" предполагается выполнение следующих мероприятий: