Таким чином, надійний захист телекомунікаційних мереж від загроз та кібератак можливий тільки на основі побудови комплексної системи безпеки інформації на всіх етапах розробки, введення в дію, модернізації апаратно-програмних засобів телекомунікацій, а також при обробці, зберіганні і передачі інформації по каналах зв'язку з широким застосуванням сучасних методів захисту інформації в бездротових мережах, яка б включала в себе взаємопов'язані заходи різних рівнів: нормативно-правового; організаційного (адміністративного); програмно-апаратного; технічного та ін.

Список використаних джерел

1. Богуш В. В., Соколов В. Ю. Дослідження захищеності Wi-Fi мереж. Зв'язок. 2009. №4 (88). С. 29–31.
2. Бурячок В. Л., Астапеня В. М., Соколов В. Ю. Способы повышения доступности информации в беспроводных системах стандарта IEEE 802.11 с MIMO. Сучасний захист інформації. 2016. №2. С. 60–68.
3. Платоненко А.В. Захист інформації у бездротових мережах WI-FI / Платоненко А.В. // Науково-технічна конференція «Актуальні проблеми забезпечення інформаційної безпеки держави» – Київ: ДУТ, 2014 – С.40-41.
4. Соколов В. Ю., Карацюба К. І. Використання дерев атак для аналізу захищеності бездротових технологій стандарту IEEE 802.11. Вісник ДУІКТ. 2012. Т. 10, №1. С. 42–49.
5. Чернобай К. Ю., Грибков С. В. Аналіз та шляхи вирішення проблем захисту комерційних бездротових локальних мереж WI-FI // Вісник національного університету "Львівська політехніка" . - № 880 (2017), с. 99-103

УДК 004.056.5

ІНФОРМАЦІЙНА БЕЗПЕКА. МЕТОДИ ПСИХОЛОГІЧНОГО ВПЛИВУ

Плакса А. О здобувач вищої освіти гр.КБ-171
Науковий керівник: **Мехед Д. Б.,** к.п.н., доцент
Національний університет «Чернігівська політехніка»

За останні роки кількість унікальних кібератак збільшувалася з кварталу в квартал та за підсумками 2020 року на 19% перевищила число кібератак в 2019 році. Найбільш часто кібератакам піддавалися держустанови, промисловість, медицина, сфера науки і освіти, фінансова галузь. На ці галузі припадає понад половини всіх кібератак на юридичні особи (54%). Частка атак на промислові компанії збільшилась до 10% проти 4% в 2019 році. Цю галузь атакують переважно з використанням шкідливого ПЗ (подібних атак 90%). Цілеспрямованих атак було істотно більше, ніж масових. Їх частка склала 73%, що на 13 % більше, ніж в 2019 році. Одна з причин - зростання числа APT-атак. Протягом року відзначалась висока активність до 27 APT-груп. Інформація як і раніше представляє високу цінність для кіберзлочинної спільноти. Частка кампаній, спрямованих на отримання даних, склала 60% і 57% в атаках проти юридичних та приватних осіб відповідно. Найбільший інтерес для зловмисників представляли персональні дані, облікові записи та дані банківських карт [3;с.158]. Загальна кількість заражень шкідливим ПЗ в 2020 році на 38% перевищила аналогічний показник 2019 року. Успіху шкідливих компаній сприяла модернізація як самого ШПЗ, так і засобів його постачання. Шифрувальники - одна з найбільш актуальних кіберзагроз для компаній по всьому світу. На їх частку припав 31% заражень ШПЗ серед юридичних осіб. Середня сума виплат в 2019- 20 роках досягла кількох сотень тисяч доларів США. Оператори шифрувальників шантажують жертв публікацією викрадених перед шифруванням даних у разі відмови платити викуп. Протягом всього року регулярно

спостерігалися атаки за допомогою JavaScript-сніферів MageCart. Вони набули масового характеру за рахунок компрометації через постачальників програмного забезпечення для веб-ресурсів (supply chain).

Був зафіксований черговий сплеск атак на медичні установи. Половину всіх інцидентів складають атаки шифрувальників, які спекулюють даними пацієнтів, позбавляють лікарні можливості працювати, відрізаючи доступ до інформаційних систем, листам призначень і оглядів. Частка атак з використанням методів соціальної інженерії, в яких зачіпається тема COVID-19, скоротилася з 16% у другому кварталі до 4% в третьому. Ми пов'язуємо це, перш за все, з тим, що люди поступово звикають до нової дійсності і тема COVID-19 вже не справляє такого сильного ефекту. До слова, якщо раніше в фішингових розсилках пропонувалися засоби захисту від вірусу, то зараз зловмисники експлуатують інтерес суспільства до вакцини. У порівнянні з минулим кварталом частка використання хакинга як метод атак на компанії збільшилася на 12 процентних пунктів і становить 30%. Ми пов'язуємо це з тим, що зловмисники продовжують шукати уразливості в сервісах на периметрі корпоративних систем. У зв'язку з пандемією та переходом на віддалену роботу багато компаній вивели на периметр додаткові сервіси, які не завжди виявляються надійно захищені; таким чином, у злочинців з'явилося більше можливостей для атак. Крім того, системи, що використовуються для організації віддаленого доступу, бувають схильні до відомих вразливостей, і ми бачимо, що ці вразливості активно експлуатуються. У липні повернувся і вже отримав статус найактуальнішої загрози троян Emotet. У робочі дні розсилається більше 500 тисяч листів, що містять цей шкідливий контент. Він краде потрібну йому інформацію і передає доступ у внутрішню мережу організації операторам програм-вимагачів та банківських троянів.

Підсумовуючи дану інформацію, можна зробити висновок, що велика кількість випадків інформаційної безпеки пов’язана з психологічними впливами на такі об’єкти атак як:

- Комп’ютери, сервери та мережеве обладнання;
- Веб – ресурси;
- Люди;
- Банкомати та POS – термінали;
- Мобільні пристрої;
- IoT (Internet of Things) пристрої.

Вважаємо за доцільне проаналізувати методи психологічних впливів та виявити найбільш поширеніші з них.

З точки зору фізичної сутності принципів та механізмів впливу, засоби та методи інформаційно-психологічних впливів можуть бути класифіковані в такий спосіб:

- переконання і сугестивні методи;
- інформаційно-техногенні;
- психотропні (фармакологічні);
- «феноменологічні» (екстрасенсорне зцілення, шкірний зір, телекінез, ясновидіння та ін.); - комбіновані - комбінації перерахованих вище.

а) переконання є методом відкритого вербального (словесного) інформаційно-психологічного впливу на свідомість індивіда або групи людей, основу якого становить система прозорих, чітко сформульованих аргументів, збудованих за законами формальної логіки та обгрунтованих висуваємим суб'єктом впливу тез (точок зору). В результаті аналізу та оцінки цих тез об'єкт впливу з ними погоджується або відкидає їх. Переконання є найетичнішим засобом інформаційно - психологічного впливу, тому що тут немає грубого насильства або підступного впровадження в підсвідомість об'єкта. Через практичне виконання, переконання являє собою чітку, інколи й приховану дискусію (бесіду), що доповнюється деяким стимулюючим впливом.

Сугестія (лат. suggestio - вплив, натяк) або навіювання - це процес неаргументованого інформаційно-психологічного впливу на свідомість людини, пов'язаний зі зниженням критичності при сприйнятті та реалізації ним змісту інформації, що повідомляється, з відсутністю активного її розуміння, осмислення, розгорнутого логічного аналізу і оцінки в

співвідношенні з минулим досвідом. На відміну від переконання, навіювання грунтується не на логіці та розумі людини, а на її здатності сприймати слова іншої особи як належне, як інструкцію до дії. При навіюванні спочатку відбувається сприйняття інформації, що містить готові висновки, а потім на її основі формуються мотиви та життєві установки певної поведінки [1;с.78].

б) До інформаційно-техногенних засобів та методів інформаційно - психологічного впливу відносяться: інформаційні та технічні психотехнології з використанням телевізійної, обчислювальної, радіомовної техніки, аудіо-, відео-, друкованої та кінопродукції; генератори спеціальних випромінювань; акустичні системи з «Інтелектуальним» сигналом (включаючи інфразвук і ультразвук); оптичні засоби у видимому, інфрачервоному й ультрафіолетовому діапазонах; біорезонансні системи. Інформаційно-психологічний вплив за допомогою цих засобів та методів досягається за вектором «техніка - людина» та найбільш широко - через засоби масової інформації.

в) До психотропних (грец. psyche - душа, свідомість + tropos - поворот, напрям) засобів (речовин) інформаційно-психологічного впливу відноситься група біологічно активних речовин, які значно впливають на психічні функції людини (в тому числі на емоції та поведінку), а також здатних переводити її в змінений стан свідомості. Під дією психотропних засобів індивід може прийняти рішення, вигідне іншій людині. Психотропні засоби отримують або в результаті хімічного синтезу, або з певних рослин.

г) парапсихологія (грец. para - біля, поза, psyche - душа і logos - слово, вчення). Предметом вивчення парапсихології вважають біополя і явища психофізичної взаємодії - паранормальні явища, до яких відносяться: екстрасенсорна перцепція (сприйняття властивостей об'єктів, їх стану без фізичного контакту з ними і без використання звичайних органів почуттів); телекінез або психокинез (уявний або безконтактний вплив людини на фізичні об’єкти або події, грец. psiche - душа + kineos - рух); екстрасенсорне цілительство (функціональна діагностика та терапевтичний вплив за допомогою біоенергоінформаційних взаємодій); телепатія (сприйняття однією особою думок і почуттів іншої особи без використання будь-яких відомих сенсорних каналів, грец. tele - відстань, далеко + pathos - сприйняття, почуття); ясновидіння (сприйняття подій з сьогодення, минулого і майбутнього, невидимих віддалених об'єктів без використання органів почуттів); біолокація та інші явища.

д) під комбінуванням засобів (методів) інформаційно-психологічного впливу будемо розуміти практично одночасне застосування двох і більше засобів (методів) такого впливу. Найбільш відомим і простим прикладом комбінування засобів і методів інформаційно-психологічного впливу є комплексне використання аудіо- та відеосугестії. Вже доведено на практиці, що неусвідомлюване акустичне навіювання, що супроводжує зорову усвідомлювану інформацію, може модулювати ставлення до останньої. Наприклад, при демонстрації людського обличчя піддослідні оцінювали його як образ людини поганої або хорошої в залежності від настанови, яка формується у них за допомогою одночасно з неусвідомлюваним акустичним навіюванням. Таким шляхом можна модулювати ставлення, наприклад, до тієї чи іншої телевізійної інформації. Ефективним прийомом модифікації свідомості та поведінки людини можуть з'явитися кольорово - музичні впливи, які організовані певним чином [2;с.67].

Для захисту від кібератак, перш за все, треба дотримуватися загальних рекомендацій щодо забезпечення особистої і корпоративної кібербезпеки. У світлі нових тенденцій грамотно вибудований процес управління вразливостями стає не просто відповіддю на вимоги регулятора або на рекомендації галузевого стандарту, а одним із пріоритетних потреб для корпоративної служби ІБ. Крім ефективного процесу управління вразливостями, необхідно використовувати сучасні засоби захисту, включаючи WAF, засоби аналізу трафіку, SIEM-системи. Для запобігання атак, пов'язаних з доставкою шкідливих програм по електронній пошті, слід перевіряти вкладення у спеціальному віртуальному середовищі, призначеному для поведінкового аналізу файлів.

Список використаних джерел

1. Ложкін Г. Інфомаційна безпека. Методи психологічного впливу [Електронний ресурс] / Г. Ложкін // Персонал. – 2003.
2. Толубко В. Б. Інфомаційна безпека. Методи психологічного впливу [Електронний ресурс] / В. Б. Толубко // Навчальний посібник. К. :НАОУ. – 2002..
3. Юдін О. К. Інфомаційна безпека. Методи психологічного впливу [Електронний ресурс] / О. К. Юдін // Навчальний посібник. Х.: Консум. – 2005..

УДК 004.056.55

СУЧАСНА КРИПТОГРАФІЯ. СИМЕТРИЧНЕ ТА АСИМЕТРИЧНЕ ШИФРУВАННЯ

Сич К. В., здобувач вищої освіти гр. КБ-181
Науковий керівник: **Семедяй С. М.,** викладач
Національний університет «Чернігівська політехніка»

До алгоритмів симетричного шифрування належать методи шифрування, в яких і відправник, і отримувач повідомлення мають однаковий ключ (або, що менш поширено, ключі різні, але споріднені та легко обчислюються). Ці алгоритми шифрування були єдиними загально відомими до липня 1976.

Сучасні дослідження симетричних алгоритмів шифрування зосереджено, в основному, навколо блочних та потокових алгоритмів шифрування та їхнього застосування. Блочний шифр подібний до поліалфавітного шифру Альберті: блочні шифри отримують фрагмент відкритого тексту та ключ, і видають на виході шифротекст такого самого розміру. Оскільки повідомлення зазвичай довші за один блок, потрібен деякий метод склеювання послідовних блоків. Було розроблено декілька методів, що відрізняються в різних аспектах. Вони є режимами дії блочних шифрів та мають обережно обиратись під час застосування блочного шифру в криптосистемі [1].

Шифри Data Encryption Standard (DES) та Advanced Encryption Standard (AES) є стандартами блочних шифрів, затверджених урядом США (однак, стандартизацію DES було скасовано після прийняття стандарту AES). Не зважаючи на те, що стандарт DES було визнано застарілим, він (та особливо його все ще дійсний варіант triple DES) залишається досить популярним; він використовується в багатьох випадках, від шифрування в банкоматах до забезпечення приватності електронного листування та безпечного доступу до віддалених терміналів. Було також розроблено багато інших шифрів різної якості. Багато з них було зламано.

Потокові шифри, на відміну від блочних, створюють ключ довільної довжини, що накладається на відкритий текст побітово або політерно, в дечому подібно до одноразової дошки. В потокових шифрах, потік шифротексту обчислюється на основі внутрішнього стану алгоритму, який змінюється протягом його дії. Зміна стану керується ключем, та, в деяких алгоритмах, ще і потоком відкритого тексту. RC4 є прикладом добре відомого, та широко розповсюдженого потокового шифру.

Криптографічні гешувальні функції (англ. cryptographic hash functions, або англ. message digest functions) не обов'язково використовують ключі, але часто використовуються і є важливим класом криптографічних алгоритмів. Ці функції отримують дані (часто, ціле повідомлення), та обчислюють коротке, фіксованого розміру число (хеш). Якісні хешувальні функції створені таким чином, що дуже важко знайти колізії (два відкритих тексти, що мають однакове значення хешу).

Коди автентифікації повідомлень (англ. Message authentication code, MAC) подібні до криптографічних хешувальних функцій, за винятком того, що вони використовують секретний