На правах рукопису

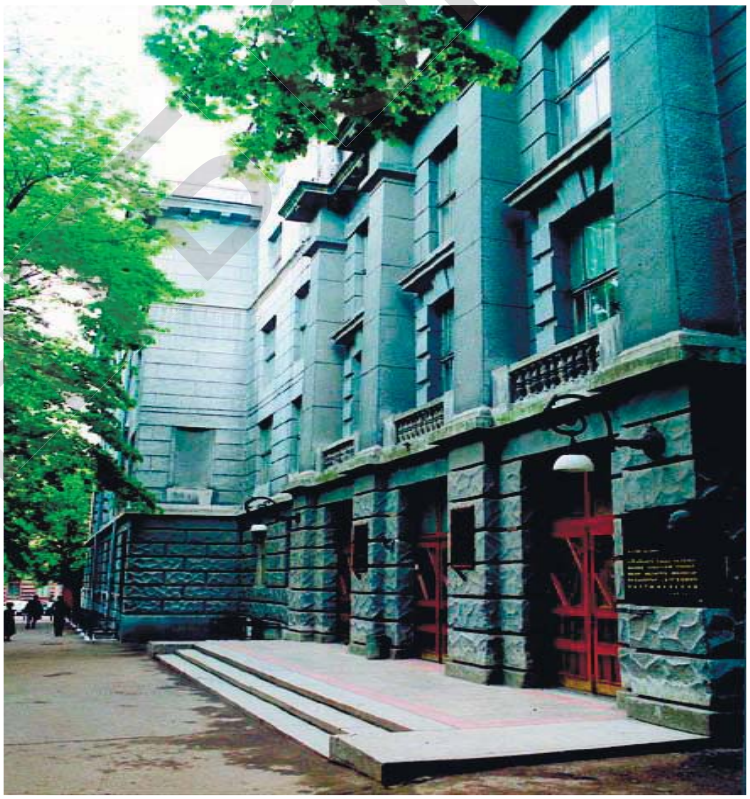
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут комп'ютерних систем і технологій
«Індустрія 4.0» ім. П.М. Платонова
Факультет комп'ютерної інженерії, програмування та кіберзахисту

XVIII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

"СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ"

Матеріали конференції. Частина І



Одеса
19 квітня 2018 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVIII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 19 квітня 2018 р. - Одеса, Видавництво ОНАХТ, 2018 р. - 96 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова – д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови :

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНАХТ,
Котлик С.В. – к.т.н., доц., в.о. директора ННІКСіТ "Індустрія 4.0" ОНАХТ,
Даріуш Долива – д.м.н., уповноважений декана факультету Інформатики УІтаПЗ, м. Лодзь, Польща,
Ковалюк Т.В. – к.т.н., доц. кафедри АСОІтаУ НТУУ «Київський політехнічний інститут»,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Члени оргокомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНАХТ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНАХТ,
Князєва Н.О. – д.т.н., проф. кафедри КІ ОНАХТ,
Ломовцев П.Б. – к.т.н., доц., в.о. декана ФКІПтаК ОНАХТ,
Волков В.Е. – д.т.н., проф., завідувач кафедри ПМіП ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНАХТ,
Шамрай О.А. – к.т.н., доц., заступник декана ФКІПтаК ОНАХТ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

характеристики між користувачами за допомогою лінійної залежності між двома елементами. Алгоритм кластеризації базується на виділенні подібності між елементами (користувачами) шляхом обчислення їх близькості один одному в так званому просторі ознак. Ознаками виступають ті елементи, за якими сходяться інтереси певних учасників процесу (для музичних ресурсів – це треки, для кіно-порталів – фільми). Схожі по характеристикам користувачі об'єднуються в так звані кластери.

Мета роботи – урахувати усі недоліки і переваги існуючих аналогів систем рекомендацій, основуючись на головних методах, прийомах і алгоритмах, для розробки власної системи рекомендацій, яка буде основана на перевагах користувачів.

ПРИНЦИПЫ МНОГОУРОВНЕВОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Щербина Р.В., студентка, ОНАПТ, Одесса

Защита передаваемой и хранимой информации в настоящее время базируется на принципах, разработанных в криптографии и стеганографии. С помощью криптографических методов защищаемое сообщение преобразуется в набор символов, нечитаемый без ключа. Приёмы стеганографии позволяют создать скрытый канал связи, который сложно обнаружить даже с помощью специальных методов обработки информации [1, 2, 3]. Распределение скрываемой информации в контейнерах происходит по секретному ключу.

Специалистами проведено большое число результативных криптографических атак на известные шифры и на стеганографические методы защиты. Наличие успешно проведённых атак говорит о имеющейся уязвимости существующих принципов защиты информации.

Процесс разработки средств защиты информации и средств атаки на шифры и методы сокрытия сообщений носит соревновательный (итерационный) характер. Как правило, через несколько лет после создания широко распространённого шифра появляется эффективная атака на этот шифр и его использование постепенно затухает.

Принципиально новым подходом к защите информации может стать метод формирования нескольких уровней защиты сообщений (см. рисунок 1).

Одним из дополнительных барьеров защиты (помимо криптографического и стеганографического) может стать пространственное распыление защищаемой информации.

Основная идея пространственного распыления информации состоит в том, что сообщение дробят на возможно мелкие составляющие (предложения, слова, символы, блоки символов, группы байт, байты, группы бит, биты) и передают частями, распределяя их по нескольким каналам связи.

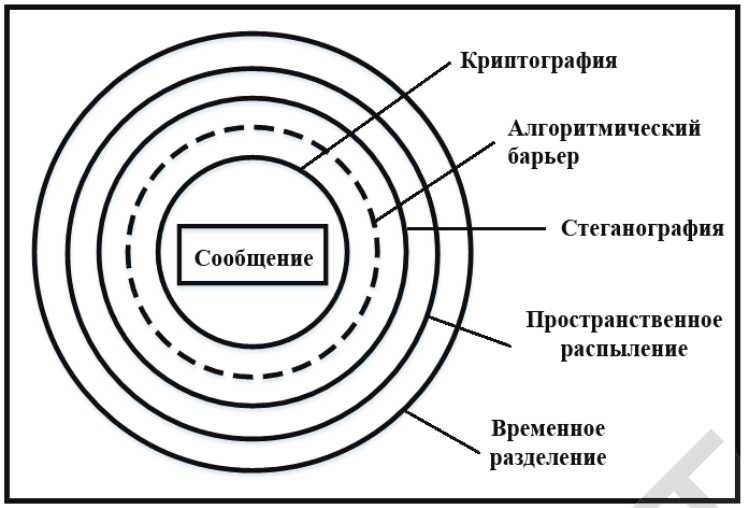


Рисунок 1 - Пять барьеров защиты

Помимо трёх перечисленных уровней защиты передаваемой информации можно создать ещё один уровень (четвёртый), который технически и алгоритмически гармонично сочетается с ранее рассмотренными барьерами. Это - временное разделение сообщения (передача данных по заранее согласованному расписанию). Пространственное и временное разделение сообщения удачно сочетаются между собой, дополняя друг друга. Эти два барьера можно представлять в виде единого барьера и назвать его пространственно-временным распылением сообщения.

Пятый (алгоритмический) барьер базируется на таком способе обработки передаваемых блоков криптограммы, при котором отсутствие хотя бы одного перехваченного блока вызывает у криптоаналитика труднопреодолимые вычислительные сложности. Пятый барьер как бы является продолжением криптографического барьера, однако методологически его целесообразно выделить в отдельный уровень защиты.

Таким образом, путём создания множества барьеров разного вида можно осуществить принцип комплексной, многоуровневой защиты информации. В каждом конкретном случае стороны обоснованно выбирают достаточную степень защищённости сообщения (число используемых барьеров, вид шифра, длину ключа, виды стеганографических контейнеров, способы стеганографического внедрения информации в контейнеры, вид и число ис-пользуемых каналов связи или носителей хранения информации, количество временных окон для передачи информации). Реализация предлагаемых мер повышения криптостойкости сопровождается увеличением времени передачи сообщения, числа ошибок при передаче сообщения, усложняет процедуру передачи, снижает удобство хранения информации. Регулировать степень защиты сообщения (значит, и варьировать время передачи сообщения, изменять сервисные свойства) можно путём выборочного использования не всех барьеров, а только достаточной их части. Оперативная передача информации (когда ценность информации исчисляется часами и даже минутами) может происходить при минимальном числе используемых барьеров.

Список литературы

1. Алексеев А.П. Многоуровневая защита информации. Самара: ПГУ-ТИ-ИУНЛ, 2017. – 128 с. ISBN 978-5-904029-72-2
2. Повышение уровня информационной безопасности [Электронный ресурс] / https://revolution.allbest.ru/programming/c00734328.html

СИСТЕМА МОНІТОРИНГУ ТА ЖУРНАЛЮВАННЯ РЕСУРСІВ МЕРЕЖІ

Юмін О.В., студент 4-го курсу групи 341-б ОНАХТ,
Селіванова А. В., к.т.н., доцент КІТКБ ОНАХТ

У наш час люди мають потребу зберігати величезну кількість інформації. Це може бути особиста інформація або дані що є результатом довгої праці. Сучасні технології допомагають звільнити людство від потреби складати шукати місце для купи паперів із записами. Усю інформацію можна завантажити до персонального комп'ютера який є майже у кожній хаті. Комп'ютер не лише допомагає зберігати інформацію, він також в рази спрощує процес її передачі від одного користувача до іншого. Це стає можливим за допомогою підключення до мережі Інтернет, але, нажаль разом із підключенням виникає загроза втрати чи викрадання особистої інформації та даних. З кожним роком зловмисники вигадають нові способи виламати систему для викрадення чи знищення інформації.

В світі вже існують різноманітні способи захисту інформації, які можна класифікувати як показано нижче:

- засоби захисту від несанкціонованого доступу (засоби авторизації, мандатне керування доступом, виборочне управління доступом, управління доступом на основі ролей, журналювання (аудит));
- системи аналізу та моделювання інформаційних потоків (CASE-системи).
- системи моніторингу мереж (системи виявлення й запобігання вторгнень (IDS / IPS), системи запобігання витоків конфіденційної інформації (DLP-системи);
- аналізатори протоколів;
- антивірусні засоби;
- між мережеві екрани;
- криптографічні засоби (шифрування, цифровий підпис;
- системи резервування;
- системи аутентифікації (пароль, ключ доступу (фізичний або електронний), сертифікат, біометрія);
- інструментальні засоби аналізу систем захисту (антивірус) [1].

Але, нажаль, не зважаючи на величезну способів захисту інформації та запобігання доступу, кожна система все одно вразлива до зламу. Сучасні фаєрво-