Литература

1. Общие вопросы электромагнитной совместимости в кабельных линиях передачи данных / Технологии и средства связи. [М], 2018-2019. URL: http://tssonline.ru/articles2/in-ch-sec/obsch_vopr_elektro_magn_sovmest_kabeln_lin_pereda4i_dannyx (дата обращения 20.06.2019).
2. Якимов В.Н. Обобщенная математическая модель двухуровневого знакового преобразования // Техника машиностроения, 2000. – № 4. – 72 с.
3. Rin N. Virtual Machines Detection Enhanced, 2013. – Т.55. – С.18 – 21.

УДК 004.056.5(043) **Information Control Systems and Technologies, pp. 79-82**

К.ф.-м.н. Журиленко Б.Е., Николаева Н.К.

ВЕРОЯТНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАВИСИМОСТИ ОТ ПРОЕКТИРУЕМОГО НАПРАВЛЕНИЯ ВЗЛОМА

Ph.D. Zhurylenko B., Nikolaieva N.

PROBABILITY OF PROTECTION OF INFORMATION DEPENDING ON THE PROJECTED DIRECTION OF THE BREAKING

Техническая защита информации (ТЗИ) в различных странах осуществляется в соответствие со своими нормативными документами и разрабатываемыми методами защиты. При проектировании ТЗИ параметры взлома закладываются разработчиком и должны соответствовать исходным данным.

В этом случае необходимо знать вероятностную надежность ТЗИ в проектируемом направлении взлома и в направлении реального процесса взлома.

Чтобы построить проектируемую поверхность вероятности для конкретно выбранной попытки и времени взлома, воспользуемся выражением, полученным в [1] через параметры конкретной попытки взлома, например,

$$m = m_c,\ t = t_c.$$

, (1)

где функцию $f(m,t)$ в направлении взлома в зависимости от изменения одной из координат можно представить в виде: времени

$$f(t) = \left[(m_1 - 1) + \frac{m_2 - m_1}{t_2 - t_1} \cdot (t - t_1)\right] \cdot t \quad , \tag{2}$$

и попытки взлома

$$f(m) = \left[t_1 + \frac{t_2 - t_1}{m_2 - m_1} \cdot (m - m_1)\right] \cdot (m - 1) \quad , \tag{3}$$

γ - учитывает эффективность защищенности и определяется отношением рисков вложенного финансирования в защиту к полным финансовым потерям без защиты, *P(X)* – вероятность ТЗИ от вложенного в ее построение финансирования [2].

Значения выражений, (2) и (3) равны между собой и дают значение максимума вероятности в точке взлома $f(m,t) = f(t) = f(m)$.

Чтобы построить распределение вероятности проектируемой поверхности (1) для конкретно выбранной попытки и времени взлома, в выражениях (2) или (3) необходимо выразить степень через параметры конкретной попытки взлома, например, $m = m_c$, $t = t_c$.

На рис.1а представлена поверхность с максимумом вероятности взлома в точке с выбранным направлением взлома по линии 1, например, с максимумом в точке $m_c = 10$, $t_c = 5$. А линия 2 другому реальному направлению взлома, но на поверхности, определяемой направлением взлома по линии 1.

Линия 3 дает направление реального взлома, если злоумышленник изменил реальный процесс нападения. Из рис.1а видно, что при изменении направления взлома (линии 2,3) надежность ТЗИ будет меняться и при ее проектировании необходимо это учитывать.

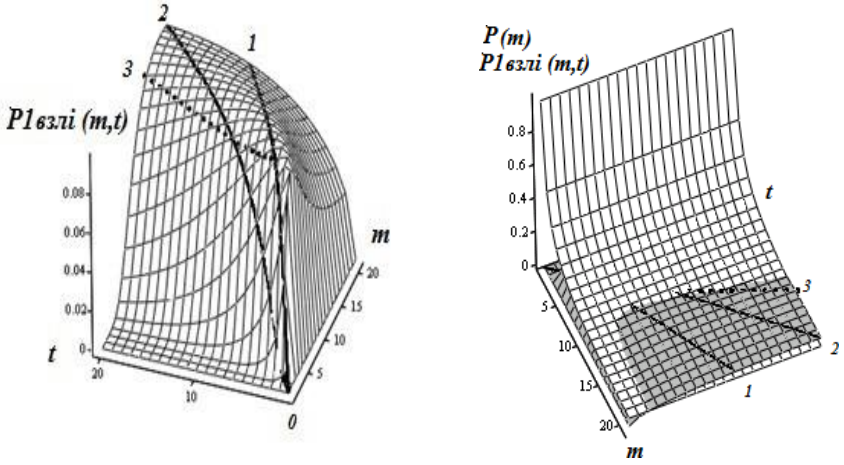
На поверхности по координатам *m*, *t* видны максимумы значений вероятностей взлома.

Точка пересечения обоих максимумов и направления линии дает точку максимума вероятности взлома в данном направлении.

Такая точка на рис.1а представлена пересечением поверхности с линией 1 проектирования направления процесса взлома с координатами $m_м = 10$, $t_м = 5$, а для линии 2 с $m_м = 12$, $t_м = 11$.

На рис.2б видно, что реальный процесс взлома, соответствующий выражению ***P(m)=1/m***, и спроектированной защиты будет проходить с

вероятностью определяемой линией пересечения белой и серой поверхностей.



а б

Рис.1. Распределение вероятности взлома: ***а*** *– с проектируемым направлением взлома по линии 1(серая поверхность);* ***б*** *– поверхность рис.* ***а*** *и реальная поверхность взлома (белая поверхность), рассчитываемая по формуле* ***P(m)=1/m***

В данном случае, согласно рис.2б, процесс взлома с расчетным максимальным значением вероятности будет только для направления проектируемой ТЗИ (линия 1), а для остальных направлений значение вероятности взлома будет меньше (линии 2 и 3).

Если направление реального процесса взлома близко к проектируемому направлению защиты, то взлом ТЗИ может произойти при значения близких к проектируемой попытке взлома $m_{взл}$, особенно при небольших увеличениях по времени между попытками взлома.

При значительных увеличениях по времени между попытками взлома, взлом ТЗИ возможен не только при большом времени и попытке взлома, но и не произойти совсем.

Аналогичная ситуация, когда взлом не произойдет, возможна, если попытки взлома будут следовать очень часто друг за другом.

Литература

1. Журиленко Б.Е. Вероятностная надежность защиты информации в зависимости от направления взлома/ Журиленко Б.Е., Николаева Н.К.//Захист інформації, 2018. – №3(20). – С. 174 – 179.

2. Журиленко Б.Е. Оценивание финансовых затрат на построение системы защиты информации/ Журиленко Б.Е.//Захист інформації, 2018. – №4(20). – С. 231 – 239.

УДК 519.7 **Information Control Systems and Technologies, pp. 82-84**

Тарабаєва Д.Д, к.ф.-м.н. Шпінарева І.М.,

ВЕЙВЛЕТ ПЕРЕТВОРЕННЯ ДЛЯ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ВІДЕОФАЙЛАХ

Tarabaieva D.D, Ph.D Shpinareva I.M.,

WAVELET TRANSFORMATIONS FOR HIDING INFORMATION IN VIDEO FILES

Один з напрямів захисту інформації пов'язано із захистом секретних даних від підслуховування неавторизованого користувача. Криптографія і стеганографія−це дві технології, які використовуються для захисту даних. Методи стеганографії мають тенденцію приховувати існування самого повідомлення.

Метою стеганографії є стійкість (до різних методів обробки зображень і стиснення) і ємність прихованих даних. Велика частина стеганографічних алгоритмів орієнтовані на відео.

У зв'язку з властивим структурі відеокадрів надмірності, відеосигнали є досить вразливими до атак, таким як усереднення кадру, підміна кадрів, видалення кадрів і атакам, пов'язаним зі статистичним аналізом кадрів.

Всі методи впровадження інформації в відео можуть бути розділені на дві великі групи: просторові і частотні відповідно до галузі застосування [1].

При цьому найбільш часто використовуються наступні перетворення: дискретне косинусне перетворення (ДКП); дискретне перетворення Фур'є (ДФП); дискретне вейвлет-перетворення (ДВП) [2].

ДКП продемонстрував свою перевагу в стисненні радіочастот в широкому діапазоні сигналів, таких як мова, телевізійні сигнали і