нововведение в сетевой безопасности, как двухфакторная аутентификация, всё равно полагается на один из факторов — пароль.

В этой связи обязательным является использование следующих требований, которые существенно повысят информационную безопасность при работе с паролями в сети Интернет:

Пароль должен быть выбран таким образом, чтобы злоумышленнику было невозможно подобрать его по словарю.

Для каждого сайта, где регистрируется пользователь, должен быть использован уникальный пароль, так как после получения пароля от одного из сайтов, где зарегистрирован пользователь, злоумышленники получат доступ к его e-mail, системе интернет-банкинга и другой частной информации.

Рекомендуется использовать длинные пароли со случайными символами разного регистра, которые будут храниться в зашифрованном виде на USB флэш-накопителе, защищенном паролем. Для шифрации данных рекомендуется к использованию решение TrueCrypt. При использовании пароля пользователь будет копировать его через буфер обмена, что позволит избежать утечки информации с помощью ПО, которое логирует нажатия клавиш.

Для работы с особо важной информацией (интернет-банкинг, оплата с помощью электронного платежного средства) рекомендуется использовать отдельный браузер, что позволит избежать кражи информации после открытия сайта, содержащего вредоносный код.

При работе с малоизвестными сайтами рекомендуется использовать одноразовые e-mail, созданные с помощью http://10minutemail.com. Через 10 минут после создания e-mail будет удалён.

Использование вышеперечисленных требований позволит существенно повысить информационную безопасность пользователя при работе в сети интернет и затруднит кражу информации третьими лицами.

ИМИТАЦИОННАЯ МОДЕЛЬ СИНХРОНИЗИРУЕМЫХ СЕТЕЙ КИНЦЕЛЯ

Н.В. БРИЧ

На сегодняшний день актуальна задача доставки секретной ключевой информации. Использование синхронизируемых искусственных нейронных сетей (ИНС) является одним из перспективных решений задачи формирования общего секретного ключа. Для изучения особенностей сетей Кинцеля создана имитационная модель на языке высокого уровня Python 3.2. Программа является консольным приложением, позволяющим анализировать свойства ИНС и моделировать основные типы атак. Результаты моделирования сохраняются в файл. Пользователь имеет возможность устанавливать значение количества необходимых испытаний. Достоинствами разработанной модели является скорость вычислений, которая соизмерима со скоростью работы программ, написанных на языке С.

АВТОМАТИЗАЦИЯ ПРОЦЕССА КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

С.М. ДОВГУЧИЦ

На сегодняшний день не существует универсальных систем обнаружения и предотвращения атак в связи с огромным разнообразием защищаемых информационных систем и ресурсов. Процесс обнаружения атак можно усовершенствовать путем комбинации различных программ обнаружения. Сложности связаны с различием типов и форматов информации на выходе таких систем. Также все тревожные события, сгенерированные системами контроля доступа к ресурсам на серверах и рабочих станциях, не отражают непосредственно атаки. Они описывают действия пользователя, работающего

с защищаемыми ресурсами. Поэтому при анализе ситуации должен учитываться контекст, в котором возникли данные тревожные события. Для анализа и обработки разных событий безопасности используется корреляция.

Корреляция событий подразумевает получение информации и её объединение по определенным алгоритмам. Это делает процедуру обнаружения вторжений управляемой и обеспечивает необходимые данные для будущего предотвращения и надлежащей реакции. Корреляция событий на крупном предприятии представляет собой трудоемкую задачу по обработке больших потоков данных. На этот случай предлагаются автоматизированные системы, которые могут объединять огромные объемы информации, устранять избыточность данных, находить нужные образцы событий и затем действовать, опираясь на собранный материал.

Для практической реализации автоматизации процесса корреляции событий безопасности предлагается использовать программное обеспечение GFI EventsManager, что позволит управлять информационной безопасностью защищаемой системы.

METHOD OF DERIVING OF FAST WALSH TRANSFORM ALGORITHMS

A.A. BUDZKO, ALMIAHI OSAMA M.H.

Method of factorization of Walsh matrices to obtain Fast Walsh Transform (FWT) algorithms is not very flexible. The number of different algorithms is not enough for different applications. Best FWT algorithms are obtained for Walsh-Hadamard transform.

Different method of deriving of FWT algorithm was proposed and this method can be modified and can be used for deriving new FWT algorithms for different ordering of Walsh functions. This method is based on representation any element of Walsh matrices in exponential form. Originally this method was demonstrated for deriving FWT in Walsh-Hadamard ordering. Let us consider of using this method and its modification for deriving FWT algorithm in Walsh-Paley ordering. The equation for Walsh-Paley transform can be expressed in an iterative form using expression for any element of Walsh function.

$$\bar{Y}(u_n,...,u_2,u_1)=\sum_{v_n=0}^{1}(-1)^{u_1v_n}\sum_{v_{n-1}=0}^{1}(-1)^{u_2v_{n-1}}...\sum_{v_1=0}^{1}(-1)^{u_nv_1}\ \bar{y}(v_n,...,v_1)$$

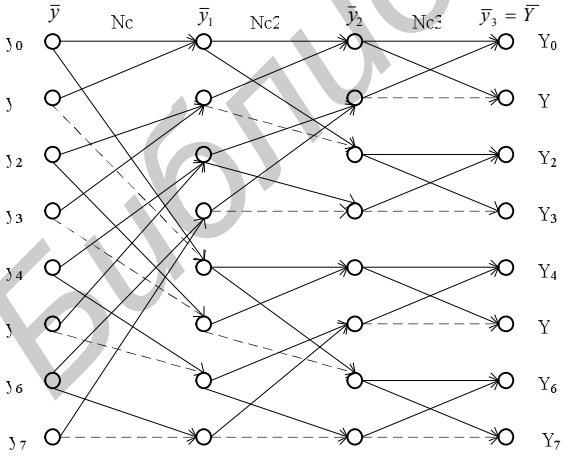

Fig.1 Signal graph of the fast Walsh-Paley transform

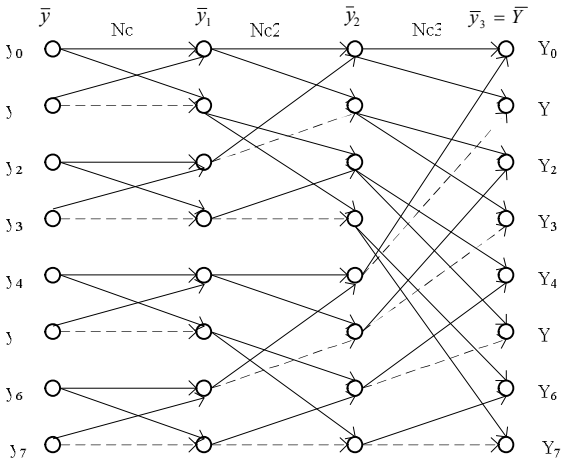

Fig.2 Signal graph of the second fast Walsh-Paley transform