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