проекта. В настоящее время CI одна из практик, применяемых в семействе гибких методологий разработки ПО.

Когда большое число разработчиков совместно работают над сложными программными проектами, интеграция разных частей кода может превратиться в длительный процесс с непредсказуемыми результатами. Однако на проектах, где процесс разработки строится на основе методик CI, проблемы и риски, связанные с интеграцией, сведены к минимуму.

В проекте, выполняемом одним человеком, интеграция ПО не является существенной проблемой, но при увеличении сложности проекта возникает необходимость в интеграции и проверке слаженной работы компонентов ПО. CI снижает трудоёмкость интеграции и делает её более предсказуемой, за счет наиболее раннего обнаружения и устранения ошибок и противоречий.

В сущности, CI гарантирует совместимость недавних изменений во вновь разработанном ПО с остальной частью ПО. На более высоком уровне CI повышает коллективную ответственность группы разработчиков и снижает трудоемкость проекта, уменьшая объем ручного труда, выполняемого при каждой интеграции.

Если описать данную методику в несколько фраз, то это: “всегда есть рабочая версия”, “автоматизированная сборка”, “всегда известно, в каком состоянии прибывает проект”.

УДК 621. 391. 25

Уязвимость алгоритма формирования общего ключа с помощью искусственных нейронных сетей к простой и геометрической атакам

Голиков В.Ф., Брич Н.В.
Белорусский национальный технический университет

Использование синхронизируемых искусственных нейронных сетей (ИНС) является одним из перспективных решений задачи формирования общего секретного ключа. Архитектура на стороне отправителя и получателя представляет собой двуслойный персептрон (TPM-архитектура), состоящий из K внутренних персептронов, каждый из которых имеет N входов. В случае простой атаки (атаки методом грубой силы) злоумышленник E знает значения входного вектора x_{ij}., выходов $Z^{\frac{A}{B}}$ на каждом шаге обучения; использует то же правило обучения, что и легитимный отправитель A (однако вместо значения Z^E использует Z^A). В случае геометрической атаки злоумышленник не пропускает итерацию,

при которой $Z^A \neq Z^B$, а корректирует значения своих весов по особому правилу. Для изучения особенностей сетей Кинцеля была разработана имитационная модель (консольное приложение) на языке высокого уровня Python 3.2. Приложение позволяет анализировать свойства ИНС и моделировать основные типы атак. Простая атака является наиболее эффективной при минимальных значениях параметров ИНС (количество персептронов, количество входов в персептрон, диапазон значений весов). При увеличении параметров N, K, L атака становится менее эффективной, однако все равно возможна ситуация, при которой $t^{AE}_{learining} \leq t^{AB}_{learining}$. Эффективность геометрической криптоатаки уменьшается с увеличением количества внутренних персептронов. Это объясняется тем, что одному выходному значению $Z^{\frac{A}{B}}$ соответствует комбинаций выходных значений внутренних персептронов $y_k^{\frac{A}{B}}$. Зависимость от диапазона значений весов и количества входов в персептрон выражена не настолько явно, однако с увеличением этих значений вероятность атаки незначительно снижается, поскольку конкретное $y_k^{\frac{A}{B}}$ может быть сформировано из нескольких комбинаций весов $w_k^{\frac{A}{B}}$.

УДК 621. 391. 25

Исследование процесса синхронизации искусственных нейронных сетей Кинцеля

Голиков В.Ф., Пивоваров В.Л.
Белорусский национальный технический университет

Искусственная нейронная сеть (ИНС) представляет собой сеть элементов (искусственных нейронов), связанных между собой синаптическими соединениями. Математической моделью нейросети является персептрон.

ИНС считаются синхронизированными, если совпадают значения векторов весовых коэффициентов персептронов сетей (изначально значения принимаются различными и случайными). Подавая на входы персептронов одинаковые случайные вектора и сравнивая между собой выходные значения, можно корректировать значения весов. В результате многократного повторения эти величины в некоторый момент времени станут равными.