**Интерактивная безопасность**

Данная технология относиться к компьютерным технологиям. Она позволяет идентифицировать пользователя посредством его взаимодействия с интерактивной виртуальной средой. Под интерактивной виртуальной средой подразумевается графическое или игровое программное обеспечение, используя которое пользователь сможет идентифицировать себя.

Из существующих подобных технологий на данный момент присутствуют паттерны разблокировки экрана, которые активно используются в аппаратных решениях безопасности, а также на мобильных устройствах. Недостаток существующих решений: однообразие паттернов идентификации, статическое изображение, возможность грубого перебора вариантов для взлома системы. Главная причина несовершенства существующих технологий идентификации пользователей – использование стандартной системы логина и пароля, которая вследствие человеческого фактора может быть взломана с помощью программного обеспечения для прослушивания сетевого взаимодействия.

Задача, которую данное предлагаемое техническое решение решает, является создание нового уровня защиты от проблемы человеческого фактора в работе комплексной системы безопасности. Современные технические средства позволяют обеспечить наивысший уровень безопасности для любого типа информационных систем. Главный недостаток заключается в том, что из-за ошибки пользователя в систему может проникнуть вредоносное программное обеспечение. Также под человеческим фактором нужно расматривать потерю мобильного устройства, посредством которого злоумышленник, зная данные аутентификации, может проникнуть в систему.

Данная задача решается в несколько этапов.

Во-первых, интерактивная безопасность позволяет произвести собственное внедрение в уже существующие решения, для создания дополнительного уровня идентификации в процессе работы с программной системой.

Во-вторых, интерактивная безопасность состоит из двух программных продуктов, которые создают закрытую программную систему безопасности используя архитектуру клиент-сервер.

При регистрации нового пользователя, система интерактивной безопасности выдает пользователю три шаблона, которые случайным образом выбираются из базы данных, находящейся на стороне сервера. Передача данных шаблонов осуществляется через защищенный шифрованный канал связи. При получении шаблонов, пользователю необходимо самостоятельно выбрать алгоритм взаимодействия с каждым из выданных интерактивных шаблонов.

Таким образом, после взаимодействия с каждым из шаблонов, на стороне пользователя система формирует шифрованный слепок его личного решения/взаимодействия с паттернами.

Для передачи шифрованного слепка, система создает 16 каналов связи с сервером, каждый из которых является отдельным потоков внутри программного обеспечения на стороне клиента. Далее шифрованный слепок разбивается на случайное к-во частей, и отправляется по заранее выбранным каналам. Выбор производиться сервером, и высылается шифрованным пакетом клиенту после установки защищенного соединения.