Труды научно–технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 10, Пенза–2016, с. 88 – 91 (http://пниэи.рф/activity/science/BIT/T10–p88.pdf)

УДК: 519.2, 612.087

Чернов П.С., Смирнов И.И., Суровцев Д.А. (г. Пенза)
Майоров А.В., Секретов М.В. (г. Пенза).

**Корпоративный интернет-портал с мобильным доступом, защищенный от сторонних вмешательств шифрованием IP-трафика и поддержкой протоколов биометрической аутентификации пользователя**

В настоящее время на рынке систем электронного взаимодействия широко представлены такие их составляющие как: система обмена сообщениями, аудио- и видеосвязь, система охранного видеонаблюдения, охранная и пожарная сигнализации, контроль и управление доступом. Классическим подходом к организации комплексной системы является объединение данных программных и технических средств в общую информационную среду и обеспечение доступа к информации с рабочих мест оператора и администратора.

Основными проблемами в данном направлении являются:

– Сложность интеграции различных подсистем в рамках единой информационной инфраструктуры. Отсутствие единых стандартов приводит к сложности организации взаимодействия технических средств различных производителей.

– Сложность реализации высокоинтеллектуальных функций (распознавание лиц, неадекватного поведения и т.п.) самими устройствами видеонаблюдения. Совместная же работа с серверной инфраструктурой обычно каждым из производителей реализуется своим способом.

– Размещение контролируемых объектов, центрального пункта наблюдения, видеоархива, сервера баз данных и других узлов системы безопасности территориально удалено друг от друга и предполагает использование открытых каналов связи и необходимости использования сертифицированных средств криптографической защиты данных, которые часто накладывают ограничения или вовсе несовместимы с используемыми аппаратно-программными комплексами.

– Поддержка различных технологий беспроводной передачи данных (Wi-Fi, 3G/4G, спутниковая связь, специализированные средства радиосвязи) с учетом требований по использованию сертифицированных средств защиты информации накладывает серьезные ограничения на технические решения.

– Резервирование канала связи и автоматический выбор оптимального на данный момент канала в условиях необходимости защиты данных.

АО ПНИЭИ помимо обширного опыта по интеграции классических подсистем, таких как видеонаблюдение, охранная сигнализация и система управление доступом, имеет многочисленные наработки по построению облачных замкнутых мультисервисных систем. Объединение технических средств в единую информационную среду может осуществляться как с помощью локальных вычислительных сетей контролируемой зоны, выделенных каналов, так и через интернет. Конфиденциальность передаваемых данных гарантируется сертифицированными аппаратными средствами криптографической защиты данных разработки АО ПНИЭИ.

Созданная мультисервисная система реализована в соответствии с принципами сервис-ориентированной архитектуры и сама является средой унифицированного взаимодействия разнородных составляющих. Подключаемым техническим средствам автоматически становится доступна вся информация, предоставляемая другими подсистемами в виде системных сервисов. Пользовательские приложения могут быть реализованы как в виде веб-интерфейса с доступом через браузер, так и в виде независимых приложений для стационарных или мобильных устройств. В связи с облачным принципом доступа к данным, взаимодействие подсистем осуществляется по стандартным протоколам сервис-ориентированной архитектуры. На рисунке 1 дана общая схема организации защищенной транспортной среды, использующей на корпоративном уровне обычные Интернет приложения.


Рис. 1. Транспортная среда с коммутацией IP- пакетов и криптографической защитой их информационного содержания

Следует подчеркнуть, что при организации защищенной корпоративной транспортной среды обмена данными, внутренняя сеть предприятия (фрагменты внутренней сети предприятия на территориально разнесенных производственных площадках) воспринимаются пользователями как обычная сеть предприятия. Доступ к ресурсам такой сети осуществляется стандартным вводом личного пароля, длина которого ограничена возможностями пользователя, а время действия определяется политикой информационной безопасности, принятой на предприятии.

При этом, как правило, пользователи должны менять свои пароли доступа через два-три месяца. Подобная практика защиты информации, к сожалению, приводит к сбоям в отлаженном технологическом процессе в момент очередной смены паролей. Администратор информационной безопасности вынужден идти на компромисс варьируя длину пароля доступа и время его действия.

Уязвимость, обусловленная малой длиной действующих паролей, и уязвимость, связанная с длительным сроком действия коротких паролей (до 3 месяцев), устраняются средствами биометрической аутентификации личности пользователя «БиоПортал».

Уязвимость коротких паролей устраняется тем, что они заменяются длинными паролями доступа, состоящими из 32 случайных знаков, получаемыми от программного генератора псевдослучайных чисел. Естественно, что такие пароли являются стойкими к атакам подбора, однако, их нельзя применять, пытаясь заставить пользователей их запомнить. Средство «БиоПортал» снимает проблему запоминания длинных случайных паролей через использование нейросетевых преобразователей биометрия-код, удовлетворяющих требованиям пакета национальных стандартов [1, 2, 3, 4, 5, 6, 7, 8, 9].

На текущий момент средство «БиоПортал» ориентировано на использование технологии анализа рукописных паролей и рисунка отпечатка пальца пользователя. Внешний вид доверенной вычислительной среды «БиоТокен» и типовых сканеров биометрии дан на рисунке 2.


Рис. 2. Внешний вид доверенной вычислительной среды «БиоТокен», выполненной в виде USB переходника между сканером биометрии и вычислительной машиной, подключенной в корпоративную сеть предприятия, через ПО средства «БиоПортал»

Особенностью использованного технического решения является то, что хранящиеся на сервере предприятия искусственные нейронные сети [1] обучаются автоматически [5]. После каждого обучения или переобучения выполняется автоматическое тестирование искусственной нейронной сети [3]. Хранение данных осуществляется в защищенных нейросетевых контейнерах [9].

Биометрия пользователя и личный ключ пользователя протокола биометрико-криптографической аутентификации не покидают доверенной вычислительной среды «БиоТокен». Фактически доверенная вычислительная среда «БиоТокен» является одним из элементов доверия, на котором строится информационная безопасность средства «БиоПортал».

Возможны два режима прошивки доверенной вычислительной среды «БиоТокен». Первый режим – это режим коллективного пользования на территории предприятия (на территории одной из производственных площадок предприятия). Второй режим – это режим личного пользования, когда сотрудник предприятия находится за его пределами в командировке. Во втором режиме доверенная вычислительная среда «БиоТокен» ориентирована на использование

только одним человеком, ранее зарегистрированном на сервере биометрической аутентификации предприятия.

Одним из новых свойств применения доверенной вычислительной среды «БиоТокен» является то, что работники предприятия утратили техническую возможность временно передать право формирования своей цифровой подписи «соседу».

ЛИТЕРАТУРА:


1. ГОСТ Р 52633.0-2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации».
2. ГОСТ Р 52633.1-2009 «Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»
3. ГОСТ Р 52633.2-2010 «Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации»
4. ГОСТ Р 52633.3-2011 «Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора».
5. ГОСТ Р 52633.4-2012 «Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код».
6. ГОСТ Р 52633.5-2011 «Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа».
7. ГОСТ Р 52633.6-2013 «Защита информации. Техника защиты информации. Требования к индикации близости предъявленных биометрических данных образу «Свой».
8. ГОСТ Р 52633.7-2017 «Защита информации. Техника защиты информации. Высоконадежная мультибиометрическая аутентификация»
9. Техническая спецификация (проект, публичное обсуждение планируется провести в 2017 году членами ТК 26 «Криптографическая защита информации») ЗАЩИТА НЕЙРОСЕТЕВЫХ БИОМЕТРИЧЕСКИХ КОНТЕЙНЕРОВ С ИСПОЛЬЗОВАНИЕМ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ.



Статья поступила 12.12.2016, опубликована 27.12 .2016 по положительной рецензии д.т.н. Иванова А.И.