ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОЕКТА «ЦИФРОВАЯ ШКОЛА». ПРОТОКОЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SSH

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бахур Н. И.

Шпак И. И. – зав.кафедрой ПЭ, канд. техн. наук, доцент

Разработан проект автоматизированной системы «Цифровая школа», позволяющий реализовать информационные технологии в школе с использованием протокола безопасности SSH.

В связи с широким внедрением информационных технологий в школьный учебный процесс современная школа резко изменяется. Использование этих технологий направлено на развитие инновационного потенциала образовательных учреждений: вовлечение педагогических работников в цифровое образовательное пространство, повышение эффективности использования современных образовательных технологий в профессиональной деятельности педагога. Региональный пилотный проект «Электронная школа» по апробации модели управляемого развития электронных образовательных услуг внедряется в Беларуси. Отдельные фрагменты «Электронной школы» уже функционируют в гимназии № 8 Витебска и СШ № 51 Ленинского района Минска.

Типовая структура «Цифровой школы» включает:

- подсистему доступа в школу, включающую задачи: «Электронная система пропуска, включающая идентификацию учащихся и поточные турникеты», «Система видеонаблюдения»;
- подсистему «Электронная организация учебного процесса», включающую задачи: «Учебные планы», «Цифровой дневник», «Электронный журнал», «Расписание занятий», «Автоматическая подача звонков между уроками», «Информационная панель» и ряд других. Одной из наиболее уязвимых в плане информационной безопасности задач проекта является задача «Цифровой дневник». Дневник должен обеспечивать конфиденциальность своей информации, доступ к которой через мобильное устройство должен предоставляться только ученику и его родителям, учителям и руководству школы (разрешённым пользователям);
- подсистему «Локальная вычислительная сеть школы»;
- подсистему «АРМы отдельных рабочих мест (делопроизводителя, бухгалтера-кассира, библиотекаря, работника медпункта, столовой (этот АРМ предусматривает безналичный отпуск завтрака и обеда в школьной столовой по электронной карте ученика) и т.д.».

Для «Цифрового дневника», используется специальное мобильное приложение, которое может установить себе каждый разрешённый пользователь. Всё, что для этого нужно – это зарегистрироваться в приложении. Приложение обеспечивает полную конфиденциальность содержащегося в нём пользовательского контента. Всю информацию, передаваемую по сети, при помощи данного приложения необходимо защищать. Для этого используются протоколы информационной безопасности. Существует множество протоколов информационной безопасности, малая часть которых распространяется бесплатно, а остальные – за деньги. На наш взгляд, недостатками платных вариантов являются:

- слабо развитый интерфейс;
- закрытость программного кода и высокая стоимость;
- платформоориентированность (под этим термином будем понимать возможность работы сервиса только в определённой операционной системе и невозможность работы в других системах;
- выполнение скриптов пользователя в назначенное время;
- отсутствие возможности автономной работы (без участия пользователя).

В докладе для защиты информации в сети школы предлагается использовать бесплатный свободно распространяемый кроссплатформенный вариант протокола ***SSH (***Secure SHell***), разработанный выпускником ИИТ [1]. Он*** является протоколом для удаленного безопасного входа и других сетевых сервисов безопасности в недостаточно надежно защищенной сети. Он состоит из трёх компонентов. Первый компонент, протокол транспортного уровня (*SSH-TRANS*) обеспечивает аутентификацию сервера, конфиденциальность и целостность соединения. Также может дополнительно обеспечивать сжатие данных. Протокол транспортного уровня обычно выполняется поверх соединения TCP, но может использоваться и поверх любого другого надежного соединения. Второй компонент, протокол аутентификации пользователя (*SSH-USERAUTH*) аутентифицирует клиента для сервера. Он выполняется поверх протокола транспортного уровня. Третий компонент, протокол соединения (*SSH-CONN*), мультиплексирует несколько логических каналов в один зашифрованный туннель. Протокол выполняется поверх протокола аутентификации пользователяВторой запрос сервиса посылается после выполнения аутентификации пользователя Протокол соединения создает каналы, которые могут использоваться для различных целей. Существуют стандартные методы установки безопасных сессий интерактивного shell и перенаправления («туннелирования») произвольных портов TCP/IP и соединений X11.

Список использованных источников:

1.Корнеев, И. А. Методы повышения надежности работы протокола SSH// 49-я науч. конф. аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии: тез. докл. (Минск, 4 мая 2013 года). – Мн.: БГУИР, 2013. – 91 с. с ил. – С. 65-66.