В.Н.АЛЕНИН[1], Н.И.БАХУР[1], В.Л.НИКОЛАЕНКО[1], И.И.ШПАК[1]

ЗАЩИТА ИНФОРМАЦИИ В ОДНОМ ИЗ ФРАГМЕНТОВ «ЭЛЕКТРОННОЙ ШКОЛЫ»

[1]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Республика Беларусь*

Информационные технологии резко меняют современное образование. В Беларуси, например, внедряется региональный пилотный проект «Электронная школа» по апробации модели управляемого развития электронных образовательных услуг. Отдельные фрагменты «Электронной школы» уже функционируют в гимназии № 8 Витебска и СШ № 51 Ленинского района Минска.

Типовая структура «Электронной школы» включает [1]: а) подсистему доступа в школу, включающую задачи: «Электронная система пропуска (идентификация учащихся и пропуск через турникеты», «Система видеонаблюдения»; б) подсистему «Электронная организация учебного процесса», включающую задачи: «Учебные планы», «Цифровой дневник», «Электронный журнал», «Расписание занятий», «Автоматическая подача звонков между уроками», «Форум школы», «Информационная панель» и ряд других; в) подсистему «Локальная вычислительная сеть школы»; г) подсистему «АРМы отдельных рабочих мест (делопроизводителя, бухгалтера-кассира, библиотекаря, работника медпункта и т. д.».

В докладе рассматривается подсистема «Электронная организация учебного процесса» и мероприятия по защите информации в ней. Доступ каждого учащегося к информационным ресурсам задач «Цифровой дневник», «Расписание занятий», «Форум школы», «Информационная панель» этой подсистемы осуществляется через свой личный мобильный гаджет (ЛМГ, смартфон или другой девайс). Предполагается, что в качестве ЛМГ будет использоваться смартфон с операционной системой Android $\geq$ 4.0 (API 14).

Выделен один из источников проникновения вредоносного программного обеспечения (ВПО) в ЛМГ учащихся – посещение ими заражённых интернет-сайтов. Попавшее в ЛМГ хотя бы одного ученика ВПО через сеть школы может заразить другие ЛМГ и всё оборудование сети. Для предотвращения такой ситуации простейшим естественным решением является блокировка доступа учащимся со своего ЛМГ к сайтам, которые могут быть заражёнными.

На основе краткого анализа возможных способов блокировки доступа в интернет и возможного использования для этого стандартного программного обеспечения в докладе предлагается:

1) использовать в качестве ЛМГ ученика специальный выделенный ему для школы смартфон (школьный ЛМГ);

2) закрыть в школьном ЛМГ доступ учащихся к информационным ресурсам интернета, оставив только доступ к вышеперечисленным задачам подсистемы «Электронная организация учебного процесса»;

3) предусмотреть в школьном ЛМГ функцию информирования через сеть и сервер школы родителей ученика о попытках доступа последнего к ресурсам интернета, неуказанным в п. 2;

4) при отсутствии у ученика отдельного школьного ЛМГ предусмотреть в его домашнем смартфоне функцию перевода родителями домашнего смартфона в ЛМГ и обратно, доверив родителям права администратора программного обеспечения домашнего смартфона их чада.

В докладе обсуждаются требования к программному обеспечению клиентской и серверной части фрагмента «Электронной школы», реализующего алгоритм защиты, изложенный в пп. 1-4. смартфона каждого учащегося.

ЛИТЕРАТУРА

1. Бахур, Н.И., Рудский, А.В., Шпак, И.И. Информационная безопасность задачи «Цифровой дневник» проекта «Цифровая школа» // Материалы XXI МНТК «Информационные системы и технологии» (ИСТ–2015), Нижний Новгород (17 апреля 2015 г.). – Нижний Новгород: Нижегородский государственный технический университет им. Р.Е. Алексеева, 2015. – С. 307.