НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИОННЫМ СИСТЕМАМ С ПРИМЕНЕНИЕМ ПРОГРАММ УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

Певнев В. Я., Кальченко В. В.

Харьковский национальный университет внутренних дел, Харьков

Специалисты в области информационной безопасности мало уделяют внимания угрозам исходящим от программ удаленного администрирования (ПУА).

Несанкционированный доступ к информационной системе с использованием ПУА может осуществляться целенаправленно (на строго определенный компьютер), либо массово (с целью получения доступа к максимально возможному числу компьютеров).

Суть проникновения заключается в том, чтобы вместе с полезной (для потенциальной жертвы) программой внедрить на его компьютер ПУА, которая будет несанкционированно использована злоумышленником. Данный метод несанкционированного доступа позволяет получить полный контроль над компьютером, при достаточно низкой вероятности обнаружения вторжения.

Методы предотвращения внедрения и использования ПУА:

– необходимо определить список повседневно используемых приложений и запретить установку/удаление любого другого ПО;

– постараться отказаться от использования нелицензионного ПО;

– по возможности заменить нелицензионное ПО на лицензионное, или использовать бесплатные версии программ;

– максимально ограничить перечень открытых сетевых портов;

– при легальном использовании ПУА использовать нестандартный номер сетевого порта и стойкий (к методу прямого перебора) пароль;

– использовать и правильно настроить брандмауэр (по крайней мере, настроить стандартный брандмауэр Windows);

– постоянно обновлять антивирусные базы;

– использовать специализированное ПО, предназначенное для защиты информации;

– осуществлять периодическую проверку компьютеров на предмет изменения параметров безопасности, перечня разрешенных программ, открытых сетевых портов;

– настройка политики безопасности ОС;

– периодическое проведение инструктажа персонала по правилам сетевой безопасности и контроль знаний.

Противодействие использованию ПУА для несанкционированного доступа к информационным ресурсам должно заключаться не только в использовании вышеописанных рекомендаций и применении программно-технических комплексов, но и постоянном обучении и контроле персонала.