УДК 004.056.5

Купцова В.Ю.

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

Белорусский национальный технический университет,
г. Минск, Республика Беларусь
Научный руководитель: ст. преподаватель Липень С.Г.

Обеспечение безопасности в компьютерных сетях – это основное условие защиты конфиденциальных данных от разного рода угроз, таких как шпионаж, уничтожение файлов, хищение информации, атака вирусами и другое. Все вышеперечисленные факторы могут негативно повлиять на корректное функционирование локальной и глобальной сети, что, в свою очередь, может привезти к разглашению или утрате конфиденциальной информации.

Самой распространенной сетевой угрозой является несанкционированный доступ извне, как умышленный, так и случайный, влекущий риск получения информации, составляющей врачебную, коммерческую, банковскую или государственную тайну.

Безопасность компьютерных сетей обеспечивается разнообразными мерами и способами, которые в зависимости от их природы можно объединить в четыре большие группы, направленные на:

1. Меры обеспечения безопасности компьютерных систем как органической части общей информационной системы предприятия.

2. Методы защиты программного обеспечения компьютеров и обрабатываемой ими информации.

3. Сетевые аспекты передачи информации между узлами компьютерной сети, безопасность сетевых протоколов и сервисов.

4. Использование технологий для защиты информации в компьютерной сети, а именно: шифрование, аутентификация, авторизация, организация защищенного канала и другие, которые в той или иной мере являются основой всех методов обеспечения безопасности компьютерных сетей.

Однако больше половины нарушений в работе сети сопряжено с неисправностями сетевого кабеля и соединительных элементов, причиной которых может быть обрыв проводов, их механическое повреждение или замыкание. Также не стоит забывать об электро-

магнитном излучении, провоцируемом бытовыми приборами, которое доставляет пользователем немало проблем.

Как правило, для установки причины и места поврежденного кабеля используют специальные сканеры, функционирование которых основано на подаче электрических импульсов с последующим контролем отраженного сигнала. Современные системы сканирования позволяют задавать номинальные параметры распространения сигнала и выводят результаты диагностики на периферийные устройства.

Защита же данных реализовывается в виде трех основных принципов информационной безопасности: идентификации, аутентификации и авторизации. Для обеспечения наибольшей безопасности способы аутентификация основывается на одноразовых и многоразовых паролях, использовании цифровых сертификатов и цифровой подписи. Авторизация осуществляется посредством мандатного, дискреционного или ролевого способов управления информацией. Также немаловажную роль играют вопросы стандартизации и сертификации средств защиты информации, многоуровневое построение политики безопасности предприятия.

Также для обеспечения безопасности сетей характерно использование криптографии, алгоритмов симметричного шифрования по методам DES и AES, а также шифрование с открытым ключом. Важнейшей технологией поддержания сетевой безопасности является технология защищенного канала, фильтрация и анализ трафика и аудит состояния сети.

Для транспортной инфраструктуры, включающей все промежуточные узлы сети, а именно: маршрутизаторы, коммутаторы, а также транспортные средства операционных систем серверов и пользовательских компьютеров, установленных в конечных узлах сети, – безопасность обеспечивается посредством разбиения сети на логические зоны, включая демилитаризованную зону и несколько внутренних зон, и защиты их с помощью файерволов и систем обнаружения вторжения. Системы мониторинга трафика на основе сниферов и агентов протокола NetFlow позволяют распознать атаку за счет выявления отклонений образцов трафика от стандартного поведения.

Важным и популярным средством обеспечения безопасности сетевых коммуникаций являются виртуальные частные сети (VPN), работающие поверх стандартной IP-сети.

Разумеется, наиболее надежными считаются комплексные способы защиты компьютерных сетей, сочетающие в себе набор мер безопасности, и чем их больше, тем лучше. В данном случае специалисты наряду с обеспечением стандартных решений разрабатывают специальные планы действий на случай возникновения нештатных ситуаций.

УДК 37.017.92

Кузьмин А.Э.

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Республиканский институт профессионального образования, г. Минск, Республика Беларусь
Научный руководитель: канд.физ.-мат.н., доцент Кравченя Э.М.

В связи с пандемией COVID-19 и высокому риску распространения острых респираторных инфекций, были приняты меры по противодействию распространения вируса в образовательной среде, прежде всего среди студентов высших учебных заведений. Одной из мер профилактики Белорусского национального университета стало применение дистанционного обучения для снижения концентрации учащихся в учебных аудиториях. Все формы организации учебного процесса (лекции, практики, лабораторные работы) были перенесены в дистанционную форму на платформе Microsoft Teams. Каждому преподавателю и студенту был присвоен уникальный логин и пароль аккаунта, после входа в который производилась его смена, тем самым соблюдалась информационная безопасность.

Дистанционное образование стало отличным выходом и решением многих проблем обучения, построило значимые традиции и модели, которые активно применяют на всех этапах образования (от школьного до высшего). Глобальное развитие и распространение информационных и коммуникационных технологий дало мощный толчок дистанционному образованию, открыло «новые горизонты», позволило осуществить «невозможное». Студент выполняет различные задания и тесты, либо слушает лекцию в домашней атмо-