УДК 681.3

СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА В КОРПОРАТИВНОЙ СЕТИ

студент гр. 113024 Дубовик Д.Г.,
кандидат техн. наук, доцент В.А. Артамонов
Белорусский национальный технический университет

Актуальность проблемы защиты информации на любом предприятии усиливается с увеличением возможностей и выполняемых функций продуктов и систем информационных технологий.

Правильно рассматривать понятие защиты информации применительно к объектам информатизации (ОИ) – носителям сведений, функционирование которых связано с обработкой, порождением, передачей и хранением электронных документов, как комплекс мероприятий, направленных на обеспечение информационной безопасности. При этом, под информационной безопасностью понимается защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий, которые могут нанести *неприемлемый* ущерб субъектам информационных отношений.

Для того чтобы защита была комплексной, необходимо:

- защитить компьютеры и всю корпоративную инфраструктуру от несанкционированного доступа (НСД) к информационным активам;
- разграничить доступ к данным, хранящимся в компьютерах;
- передавать данные только в защищённом виде;
- обеспечить неизменность технологии обработки данных.

Очевидно, что справиться с этими задачами только встроенными в ОС механизмами защиты зачастую невозможно.

Что же касается добавочных средств защиты информации (СЗИ) от НСД, то главной проблемой является выбор между программными и аппаратными средствами защиты. Однако в любом случае речь идёт о внесении добавочными средствами СЗИ НСД некоторых новых дополнительных механизмов защиты.

На основе специально разработанного профиля защиты для системы разграничения доступа в корпоративной сети предприятия показаны её возможные варианты реализации (с описанием сильных и слабых сторон). Перечислены необходимые функции (а также механизмы для их достижения), которые система ЗИ должна выполнять для достижения гарантированного уровня информационной безопасности.