7. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования / ФГУП «Стандартинформ» . – М.: «Московский печатник», 2008.
8. Луман Н. Понятие риска: Пер. с нем. // THESIS: теория и история экономических и социальных институтов и систем. — 1994. — № 5.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

***Владимир ШКВИР**, Львовская Политехника, (Украина),*
***Анджей АУГУСТЫНЕК**, Научно-технологический Университет, Краков, (Польша)*

В процессе подготовки специалистов по экономическим специальностям (бухгалтерский учет, менеджмент, маркетинг и другие), необходимо должное внимание уделять основам информационной безопасности. Это обусловлено рядом объективных причин, основными из которых являются следующие:

- деятельность экономистов, напрямую связана с формированием информационных ресурсов предприятия, часть которых попадает под действие Закона «О коммерческой тайне»;
- технологические процессы сбора, обработки и хранения информации, выполняемые пользователями, должны быть надежно защищены от несанкционированного доступа и утечки.

Предлагаемые структура и состав средств обеспечения информационной безопасности, используемые пользователями, включает следующие компоненты:

- правовые методы защиты. Пользователи должны обладать глубокими знаниями законодательного обеспечения, которое регулирует отношения в области информационных отношений. В первую очередь, это относится к Закону «О коммерческой тайне», «О персональных данных», «О бухгалтерском учете» и др.;
- организационные средства защиты;
- технические и программные средства.

Пользователи должны понимать и знать основные принципы системы информационной безопасности. Основными из них являются::

- принцип законности – заключается в соответствии принимаемых мер законодательству о защите информации, а при отсутствии соответствующих законов – другими нормативными документами по ее защите;
- принцип комплексности – с позиций предотвращения разноплановых угроз и используемых методов. Имеется в виду полнота защиты по

соответствующему методу и по перечню угроз, а также взаимовлияние методов и средств защиты;

- принцип минимальной достаточности состоит в использовании набора средств, обеспечивающих выполнение комплекса установленных требований по защите информации при заданной степени риска ее нарушения. При этом необходима увязка функционирования различных средств защиты по месту и времени, хранения и преобразования информации;
- принцип обоснованности. Под названным принципом подразумевается наличие достаточных доказательств актуальности выдвинутых требования или оценка риска нарушения защиты информации;
- принцип тактической организации защиты – предусматривает необходимость упреждающих действий в виде методов предотвращения, а не ограничения последствий. Данный принцип объединяет
- саморегулируемость сложности защиты (структурированность, позволяющая использовать более простые методы для оперативного контроля и наращивания ресурсов при возникновении угрозы для ее максимального отражения);
- автотестируемость (выполнение контроля правильности функционирования системы защиты, возможность самообучения с адаптацией и моделируемостью ситуаций);
- принцип непрерывности состояний во времени и пространстве, предполагающий невозможность функционирования объекта при исключении защиты;
- принцип восстановления нормальной работы системы.

В рамках отдельной темы необходимо рассматривать состав и структуру информационных угроз по отношению к производственно-хозяйственной деятельности фирмы (предприятия). Немаловажным является ознакомление с методиками определения экономической эффективности мероприятий по обеспечению информационной безопасности, расчетом инвестиционной привлекательности системы информационной безопасности.

У пользователей информационных и коммуникационных технологий должно сформироваться устойчивое представление о необходимости соблюдения:

- конфиденциальности, т.е. защищенности информации от ее раскрытия без разрешения владельца. Одновременно конфиденциальность – это статус, предоставляемый данным и определяющий степень их защиты;
- целостность, т.е. защищенность точности и полноты информации и информационных ресурсов. Целостность означает также гарантированность того, что данные не были изменены, подменены или уничтожены в результате случайных или преднамеренных действий;
- доступность, т.е. возможность получения доступа к информации или информационным ресурсам за приемлемое время с возможностью выполнения операций копирования, модификации или уничтожения.

Конечной целью подготовки студентов является получение комплекса теоретических знаний и практических навыков использования информационных ресурсов. Основными задачами являются следующие:

1. Обеспечение безопасности информации должно проводиться системно и комплексно на всех этапах проектирования, внедрения и эксплуатации информационных систем.
2. Система обеспечения безопасности информационных ресурсов функционально должна перекрывать все существующие угрозы безопасности информации.
3. Система обеспечения безопасности должна быть ориентирована на тактическое опережение возможных угроз.
4. В системе безопасности должны быть разработаны механизмы восстановления нормальной работы информационной системы в случае реализации угроз.

Литература

1. Девятин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. – М.: Радио и связь, 2006.
2. Джеймс Л. Фишинг. Техника компьютерных преступлений. -М: НТ Пресс, 2008.
3. Краткий аналитический вопросник по бот-сетям в РФ 2009 год. www.securitylab.ru/analytics/370022.php
4. Информационная безопасность открытых систем: В 2 т. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия-Телеком, 2006.
5. Информационная безопасность систем организационного управления. Теоретические основы: В 2 т. – М.: Наука, 2006.

ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С. В. КАРПЕНКО
Белорусский торгово-экономический университет потребительской кооперации (Гомель, Республика Беларусь)

Развитие информационных технологий (ИТ) создает качественно новые угрозы, способные приводить к катастрофическим по своим масштабам последствиям. Организационно-правовое обеспечение информационной безопасности (ИБ) представляет собой совокупность решений, законов, нормативов, регламентирующих общую организацию работ по обеспечению информационной безопасности, создание и функционирование систем защиты информации на конкретных