Основы компьютерной безопасности – общие вопросы обеспечения информационной безопасности компьютерных систем;

Организация защита информации – вопросы, связанные с организацией защиты информации на наиболее уязвимых направлениях деятельности предприятия, таких как работа с персоналом, проведение совещаний, переговоров и выставок, работа с конфиденциальными документами;

Защита информации в вычислительных сетях – представлены современные технологии защиты вычислительных сетей, отмечены методы воздействия внутренних нарушителей на корпоративную сеть;

Основы криптографической защиты информации – общие вопросы теории криптографии, принципы построения криптоалгоритмов и сетей засекреченной связи, а также основы криптоанализа и перспективные направления развития криптографии.

Литература

1. ОСВО 1-53 01 02-2013. Образовательный стандарт высшего образования. Специальность 1-53 01 02 Автоматизированные системы обработки информации. – Минск: М-во образования Респ. Беларусь, 2013. 26 с.

ОБУЧЕНИЕ ПЕРСОНАЛА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Яковлев, П.А. Хоревко, Ю.А. Скудняков

Современные организации активно используют информационные технологии, создают необходимые условия по развитию знаний и навыков сотрудников в области информационной безопасности, что на сегодняшний день является неотъемлемой частью совершенствования профессионального уровня персонала. Согласно исследованиям более 80 % инцидентов на предприятиях в сфере информационной безопасности, в которых виноваты сотрудники, происходит в результате неумышленных действий [1]. Возникает непростая задача: как добиться того, чтобы сотрудники более внимательно относились к информационной безопасности, выполняли необходимые правила и требования. Решение данной проблемы возможно несколькими путями, однако однозначно можно сказать, что без повышения квалификации сотрудников в этой области задачу защиты информации не решить. Процесс обучения в области информационной безопасности условно можно разделить на подготовку специалистов, отвечающих за защиту информации в организации, и рядовых сотрудников. Специфика обучения различных категорий пользователей состоит в глубине и масштабности отработки тех или иных вопросов [2]. Предлагается использовать метод компьютерной симуляции в обучении. Проводится анализ и обработка инцидентов, дается оценка в соответствии с политикой исследования рисков, принятой в организации. На основании результатов анализа составляется план обучения. Погружаясь в проблемную ситуацию, обучающийся пытается найти выход из нее с помощью уже имеющихся у него знаний, навыков и ресурсов. Когда становится очевидно, что их недостаточно, он начинает самостоятельно искать новые способы действий и запрашивать дополнительную информацию. Использование такого подхода позволяет прочувствовать ценность нового знания путем проб и ошибок, получить навыки правильного использования имеющихся средств защиты и ответственности за утечку информации. Независимо от результатов симуляции персонал приобретает необходимый опыт. Благодаря этому сотрудник на эмоциональном и подсознательном уровне запоминает учебный материал и понимает важность требований к информационной безопасности.

Литература

1. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. М.: ИЦ РИОР: НИЦ ИНФРА-М, 2017. 324 с.

2. Бирюков, А.А. Информационная безопасность. Защита и нападение. М.: ДМК–Пресс, 2017. 434 с.