максимумом. Наличие многопиковой зависимости говорит о том, что в трехмерном случае возникают дополнительные факторы, влияющие на распределение напряженности электрического поля в массиве нанотрубок. Эти факторы могут быть связаны с распределением заряда в нанотрубках и экранированием электрического поля отдельной нанотрубки полями соседних нанотрубок. Исследование этих факторов требует проведения дополнительных расчетов.

Литература

1. Трубецков Д.И., Рожнев А.Г., Соколов Д.В. Лекции по сверхвысокочастотной вакуумной микроэлектронике. Саратов: Изд-во ГосУНЦ «Колледж», 1996. 238 с.

2. Fuzinatto F. Field Emission Simulations of Carbon Nanotubes and Graphene with an Atomic Model // Journal of Nanomaterials and Molecular Nanotechnology. 2014. V. 3, Iss. 4.

АНАЛИЗ МЕТОДОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ И ЗАЩИТА ОТ НЕГО

И.Г. Юруть, С.И. Леонов

Обеспечение необходимого уровня защиты информации требует не просто осуществления некоторой совокупности научно-технических и организационных мероприятий, а создания целостной системы организационных мероприятий и применения специальных средств и методов защиты информации.

Если рассмотреть проблему защиты информации в сетях в целом, то можно выделить множество способов и методов доступа к информации в АСОИ. В противовес этим способам доступа существуют специальные средства защиты информации от несанкционированного доступа (НСД). Программные средства являются важнейшей и непременной частью механизма защиты современных АСОИ, что обусловлено такими их достоинствами, как универсальность, простота реализации, гибкость, практически неограниченные возможности изменения и развития. К недостаткам программных средств относится необходимость расходования ресурсов процессора на их функционирование и возможность несанкционированного изменения.

Ни одна система защиты данных не является неуязвимой. Защищая данные и создавая политику безопасности сети, необходимо задавать вопрос: является ли защищаемая информация более ценной для атакующего, чем стоимость атаки? Ответ необходимо знать, чтобы защитится от дешевых способов атаки и не беспокоиться о возможности более дорогой атаки. Это позволит со стороны материального обеспечения более рационально подойти к вопросу защиты информации. При организации работы на ЭВМ нужно разрабатывать комплексный план защиты от угроз НСД. Необходимым компонентом этого плана защиты ЭВМ являются программные средства. Кроме того, при обеспечении безопасности ЭВМ необходимо использовать и другие возможности. Должен быть организован контроль своевременной смены пароля. Должны быть продуманы и организованы физические средства контроля. Кроме того, для организации грамотной работы сети администратор должен хорошо представлять себе существующие угрозы НСД к информации. Все это вместе позволяет добиться требуемого уровня безопасности ЭВМ.

МЕЖДУНАРОДНЫЙ ПРОЕКТ РАЗРАБОТКИ СЕРИИ УЧЕБНЫХ ПОСОБИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

А.И. Якимов, В.И. Аверченков, М.Ю. Рытов, Т.Л. Шебан

В университетах Российской Федерации накоплен значительный опыт подготовки специалистов по защите информации. В Республике Беларусь образовательным стандартом ОСВО 1-53 01 02-2013 [1] предусмотрена дисциплина «Основы защиты информации». Более того, вопросы защиты информации предусмотрены и в других дисциплинах специальности.

Совместно со специалистами Российской Федерации разрабатывается серия учебных пособий «Технологии защиты информации». Серия включает следующие учебные пособия:

Защита корпоративных данных в организации – рассмотрены общие вопросы обработки персональных данных в организации, нормативно-правовая база в области обработки и защиты персональных данных;

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.