Лабораторная работа №9

Тема: «Стандарты информационной безопасности»

Цель:

К основным нормативно-правовым документам в области информационной безопасности в РФ, кроме актов федерального законодательства и методических документов государственных органов России, относятся стандарты информационной безопасности.

Стандарт информационной безопасности – нормативный документ, определяющий порядок и правила взаимодействия субъектов информационных отношений, а также требования к инфраструктуре информационной системы, обеспечивающие необходимый уровень информационной безопасности.

ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» является национальным стандартом РФ. Настоящий стандарт идентичен международному стандарту ИСО/МЭК 15408-1:2009. Он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Поэтому этот стандарт часто называют «Общими критериями».

В нем определены инструменты оценки безопасности информационных систем и порядок их использования. «Общие критерии» содержат два основных вида требований безопасности: – функциональные – соответствуют активному аспекту защиты, предъявляются к функциям безопасности и реализующим их механизмам; – требования доверия – соответствуют пассивному аспекту, предъявляются к технологии и процессу разработки и эксплуатации.

Угрозы безопасности в стандарте характеризуются параметрами: – источник угрозы; – метод воздействия; – уязвимые места, которые могут быть использованы; – ресурсы (активы), которые могут пострадать. Для структуризации пространства требований в «Общих критериях» введена иерархия класс – семейство – компонент – элемент: – классы определяют наиболее общую, «предметную» группировку требований (например, функциональные требования подотчетности); – семейства в пределах класса различаются по строгости и другим тонкостям требований; – компонент – минимальный набор требований, фигурирующий как целое; – элемент – неделимое требование.

Практическая часть

Задача 1 Используя ГОСТ Р ИСО/МЭК 27002-2012, решить ситуационную задачу. Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек). Вам необходимо разработать комплекс мероприятий (от 10 до 20) по следующему

направлению: привлечение сторонних организаций к обработке информации. Цель: обеспечение информационной безопасности при передаче ответственности за обработку информации другой организации. Изучить разделы ГОСТ Р ИСО/МЭК 27002-2012.

Задача 2 Используя основные положения части 4, главы 70 Гражданского кодекса РФ, решить ситуационную задачу. Гражданин Смирнов А.В. создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Albert 3D» и зарегистрировал на него свои права. 15.09.2019 этот гражданин заключил договор с компанией «MosTechnology» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «MosTechnology» распространила версию программы «Albert 3D» с предварительной модификацией данного программного продукта без ведома автора. Вопрос: Имеет ли место в данной ситуации нарушение авторского права гражданина Смирнова? Ответ: согласно статьи №….

Задача 3 Используя статьи УК РФ, ответьте на вопросы после ознакомления с ситуацией. Ситуация: А.Н. Иванов, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (расширение .exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 780000 рублей. Вопросы: – Какая статья УК РФ была нарушена? – Что послужило предметом преступления? – Какие неправомерные информационные действия были совершены А.Н. Ивановым?

Задача 4 Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек). Вам необходимо разработать требования к хранению, использованию и утилизации информации для вашей организации. Цель: обеспечение информационной безопасности при хранении, обработке, передаче и уничтожении информации.

Задача 5 Проработайте требования для специалистов по подбору кадров вашей организации с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников. Цель: уведомление новых сотрудников о строгом выполнении требований по обеспечению информационной безопасности и ответственности за их нарушение.

Контрольные вопросы

1. Перечислите основополагающие документы по информационной безопасности.
2. Понятие государственной тайны.
3. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
4. Дайте характеристику Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных компьютерных программ?

6. Назовите 5 – 6 из 11 существующих функциональных требований стандарта ГОСТ Р ИСО/МЭК 15408-1-2012.

7. Для чего служит профиль защиты, согласно стандарту ГОСТ Р ИСО/МЭК 15408-1-2012?

8. Что прописано в Доктрине информационной безопасности РФ?