Автор:

Швейкин Владислав Витальевич

студент

ФГАОУ ВО «Самарский национальный исследовательский

университет им. академика С.П. Королева»

г. Самара, Самарская область

ПОЛИТИКА БЕЗОПАСНОСТИ В БАЗАХ ДАННЫХ

Аннотация*: в данной работе рассматривается понятие «политика безопасности», приводятся также основные аспекты, связанные с её реализацией и обеспечением.*

Ключевые слова*: информационная безопасность, политики безопасности, СУБД, информационная система, правила, нормы, защита.*

Основные определения

1. СУБД (система управления базами данных) – программно-аппаратный комплекс, позволяющий управлять и манипулировать базами данных.

2. Информационная система – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

Политика безопасности

Политика безопасности – совокупность документированных норм, правил, принципов и процедур, а так же практических приёмов в области безопасности, которые определяют меры по обеспечению информационной безопасности, связанной с деятельностью организации.

Только человек, который чётко осознает цели организации и условия её функционирования, может определить, какая информация подлежит защите и насколько серьёзными могут стать потери от несанкционированного доступа к информации.

После принятия политики безопасности, необходимо решить вопрос о технологии её реализации в автоматизированном контуре. Для того чтобы реализовать сформулированные в терминах естественного языка нормы и правила политики безопасности нужно использовать или разработать некоторую формальную модель, допускающее эффективное программирование на каком-либо формальном языке. На сегодняшний день наиболее распространены две базовые модели безопасности данных: дискреционная и мандатная.

Цель формализации политики безопасности для информационной системы заключается в ясном изложении взглядов руководства организации на существо угроз безопасности информации в организации и технологий обеспечения информационной безопасности ресурсов системы. Политика безопасности, как правило, заключается в формулировании общих принципов и описания конкретных норм и правил работы с ресурсами информационной системы.

Политика безопасности должна быть утверждена документально на нескольких уровнях управления. На уровне управляющего звена руководства необходимо подготовить и утвердить документ, определяющий цели политики безопасности, структуру и перечень решаемых задач и ответственные за реализацию политики. Основной документ должен быть конкретизирован администраторами безопасности информационной системы с учётом деятельности организации, соотношения важности целей и наличия ресурсов. Детальные решения должны ясно определять методы защиты технических и информационных ресурсов, а так же инструкции, которые описывают поведение сотрудников в конкретных ситуациях.

Руководство по компьютерной безопасности, разработанное национальным институтом стандартов и технологий США, рекомендует включать в описание политики безопасности разделы:

1. Предмет политики. В разделе описываются цели и причины разработки политики и её область применения. Должны быть сформулированы задачи, которые решаются с использованием информационных систем, затрагиваемых

данной политикой. Так же могут быть сформулированы определения и термины, которые будут использоваться в последующих разделах.

2. Описание позиции организации. В этом разделе должен быть определён характер информационных ресурсов организации, перечень лиц и процессов, которые имеют доступ к информационным ресурсам, а так же порядок получения доступа к ресурсам информационной системы.

3. Применимость. В разделе определены ограничения или технологические цепочки, которые применяются при реализации политики безопасности, а так же может быть уточнён порядок доступа к ресурсам информационной системы.

4. Роли и обязанности. В данном разделе определены лица, которые отвечают за разработку и внедрение различных элементов политики, а так же их обязанности.

5. Соблюдение политики. В разделе описываются права и обязанности пользователей информационной системы. Необходимо явно описать и документировано ознакомить пользователей с недопустимыми действиями при осуществлении доступа к ресурсам системы и наказание за нарушение режимных требований.

Заключение

Для эффективной реализации политики безопасности необходимо, чтобы она была понятна всем пользователям информационных систем организации. Сотрудники организации должны быть обучены или ознакомлены с конкретными правилами и технологиями доступа к ресурсам информационной системой.

Список литературы

1. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.