СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В РОССИИ

LOGO

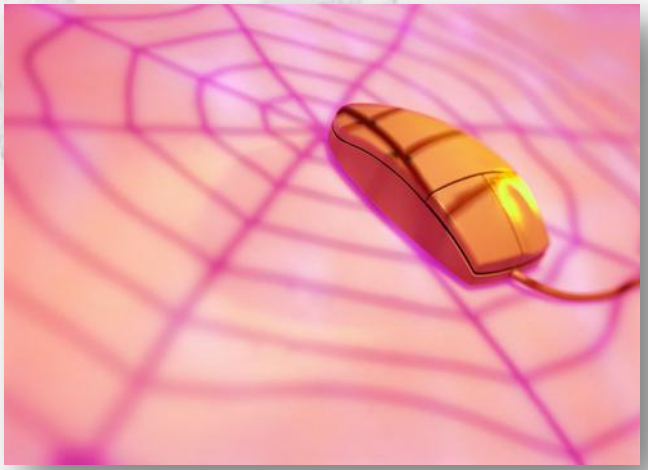
Т.А. Балышкова
СОШ №1 г. Чулым Новосибирской обл.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В РОССИИ

это организованная совокупность специальных законодательных и иных нормативных актов, органов, служб, методов, мероприятий и средств, обеспечивающих безопасность информации от внутренних и внешних угроз.

ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Комплексность.



Предполагает:

а) обеспечение безопасности обслуживающего персонала, материальных и финансовых ресурсов от всех возможных угроз всеми доступными законными средствами, методами и мероприятиями;

б) обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, во всех технологических процессах и операциях их создания, обработки, использования и уничтожения;

в) способность системы защиты информации к развитию и совершенствованию в соответствии с изменяющимися внешними и внутренними условиями.

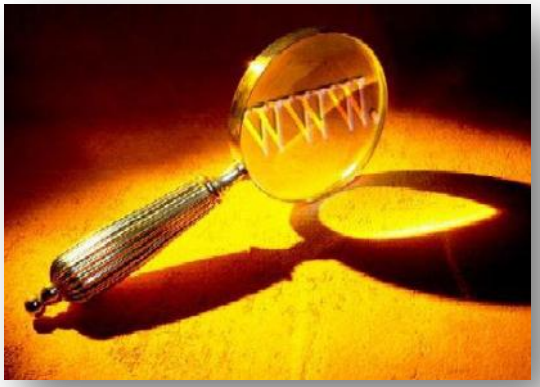
2. Своевременность

– упреждающий характер мер защиты информации. Предполагает постановку задач по комплексной защите информации на стадии проектирования (создания) системы ее защиты на основе анализа известных и прогнозирования возможных угроз безопасности информации, которые могут появиться в будущем после запуска системы защиты в эксплуатацию (реализацию).

3. Непрерывность

– постоянное поддержание работоспособности и развитие системы защиты информации.

4. Активность



– настойчивость в достижении целей и задач защиты информации. Предполагает постоянный маневр силами и средствами защиты информации, а также принятие нестандартных мер защиты.

5. Законность

– разработка системы защиты информации на основе действующего законодательства, а также иных нормативных актов, регламентирующих безопасность информации. В ходе последующей реализации системы защиты информации – применение всех законных методов и средств обнаружения и пресечения правонарушений в области безопасности информации.

6. Обоснованность.

Заключается в том, что все методы и средства защиты информации должны быть научно обоснованными и современными, соответствовать последним достижениям науки и техники. В своей совокупности они должны отвечать всем установленным требованиям и нормам по защите информации.

7. Экономическая целесообразность –

затраты на разработку и реализацию (обеспечение заданных параметров) системы защиты информации не должны превышать размеры потенциального ущерба, который может наступить в результате нарушения безопасности защищаемой информации.

8. Специализация.

Предполагает привлечение к разработке и внедрению методов и средств защиты информации специализированных субъектов, имеющих государственную лицензию на определенный вид деятельности в сфере оказания услуг по защите информации. Применяемые ими средства защиты информации должны быть сертифицированы по требованиям безопасности информации.

9. Взаимодействие и координация деятельности.

Предусматривает организацию четкого взаимодействия между всеми субъектами защиты информации, действующими в рамках единой системы защиты информации, а также координацию их усилий и осуществляемых работ в этой сфере для достижения общих целей. Заключается в интеграции и последовательности деятельности по защите конкретных информационных ресурсов.

10. Совершенствование.

Предусматривает совершенствование и разработку новых законодательных, организационных и технических мер защиты информации под воздействием объективных и субъективных факторов.

11. Централизация управления.

Предполагает наличие единого координационного центра (субъекта), занимающегося общими вопросами управления системой защиты информации, а также единых требований по обеспечению безопасности информации