Памятка по информационной безопасности в виртуальном пространстве

Информационная безопасность — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере. Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

- ***Конфиденциальность: Обеспечение доступа к информации только авторизованным пользователям.***
- ***Целостность: Обеспечение достоверности и полноты информации и методов ее обработки.***
- ***Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.***

Безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.


Межсетевое экранирование
Firewall
Криптографическая защита
Информационная безопасность
Предотвращение сетевых вторжений
IDS/IPS
Защита передачи данных в VPN
2-х факторная аутентификация пользователей

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами случайных воздействий при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характерны тем, что против них предпринимают так называемые удаленные атаки. Нарушитель может находиться за тысячи километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

Несмотря на то, что современные ОС для персональных компьютеров, такие, как Windows 2000, Windows XP и Windows NT, имеют собственные подсистемы защиты, актуальность создания дополнительных средств защиты сохраняется. Дело в том, что большинство систем не способны защитить данные, находящиеся за их пределами, например при сетевом информационном обмене.

Аппаратно-программные средства защиты информации можно разбить на пять групп:

1.Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.

2.Системы шифрования дисковых данных.

3.Системы шифрования данных, передаваемых по сетям.

4.Системы аутентификации электронных данных.

5.Средства управления криптографическими ключами.

Информация - это ресурс. Потеря конфиденциальной информации приносит моральный или материальный ущерб. Условия, способствующие неправомерному овладению конфиденциальной информацией, сводятся к ее разглашению, утечке и несанкционированному доступу к ее источникам. В современных условиях безопасность информационных ресурсов может быть обеспечена только комплексной системной защиты информации. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

Акты федерального законодательства:

- *Международные договоры РФ;*
- *Конституция РФ;*
- *Законы федерального уровня (включая федеральные конституционные законы, кодексы);*
- *Указы Президента РФ;*
- *Постановления Правительства РФ;*
- *Нормативные правовые акты федеральных министерств и ведомств;*
- *Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.*

Государственные органы РФ, контролирующие деятельность в области защиты информации:

Комитет Государственной думы по безопасности; Совет безопасности России;Федеральная служба по техническому и экспортному контролю (ФСТЭК России);Федеральная служба безопасности Российской Федерации (ФСБ России);Федеральная служба охраны Российской Федерации (ФСО России); Служба внешней разведки Российской Федерации (СВР России);Министерство обороны Российской Федерации (Минобороны России);Министерство внутренних дел Российской Федерации (МВД России);Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);Центральный банк Российской Федерации (Банк России).

Службы, организующие защиту информации на уровне предприятия

Служба экономической безопасности;Служба безопасности персонала (Режимный отдел); Кадровая служба;Служба информационной