7. Безопасность, развитие и использование данных как основы цифровых, интернет- и смарт-технологий[1].

8. Справедливая и рациональная система управления киберпространством, направленного на достижение сбалансированного отражения интересов всех стран-участников.

9. Создание интернет-цивилизации как ключевого объекта в системе прогрессивного развития человечества.

10. Совместное построение и развитие инфраструктуры Интернета для цифрового разрыва между странами и различными социальными группами населения, усиление цифровой помощи его уязвимым слоям.

Орлова Д.Е., Рябчикова Е.А.

Воронежский институт ФСИН России

Обеспечение безопасности телекоммуникационных систем

Распространение телекоммуникационных систем усугубило проблему их безопасности, особенно в отношении защиты передаваемой информации. Утечка ценной информации, например финансовой, может привести к катастрофическим последствиям для владельцев. Из-за стремительного роста ИТ появляются следующие проблемы с информационной безопасностью: использование общедоступных почтовых доменов, недостаточное антивирусное обеспечение и низкая культура ИБ. Помимо этого, угрозы могут исходить от устаревших технологий. Поэтому главной задачей становится надежная защита передаваемых данных, а не только качество и скорость передачи.

При создании новых сетей важно использовать передовые IT-решения для обеспечения необходимого уровня защиты. Защита информации включает комплекс мер против хищения данных, что решается через внедрение норм, таких как ГОСТ-Р 50922-96. Однако развитие технологий требует постоянного совершенствования методов защиты от хакерских атак и обновления стандартов.

Нарушения конфиденциальности и целостности информации могут привести к серьезным последствиям. Ущерб чаще всего связан с утечкой данных, предназначенных для ограниченного круга лиц. Поэтому обеспечение безопасности включает использование надежных технических средств, антивирусов и квалифицированного персонала.

[1] Подр.: Управление информационной безопасностью : учебное пособие / В.А. Минаев, Е.С. Поликарпов, В.Т. Еременко, М.Ю. Рытов. М.: МосУ МВД России имени В.Я. Кикотя, 2022. 310 с.

Информационная безопасность телекоммуникационных систем подвержена множеству угроз, включая вирусное заражение и нормативно-правовые коллизии. Основные виды угроз представлены на рисунке 1.

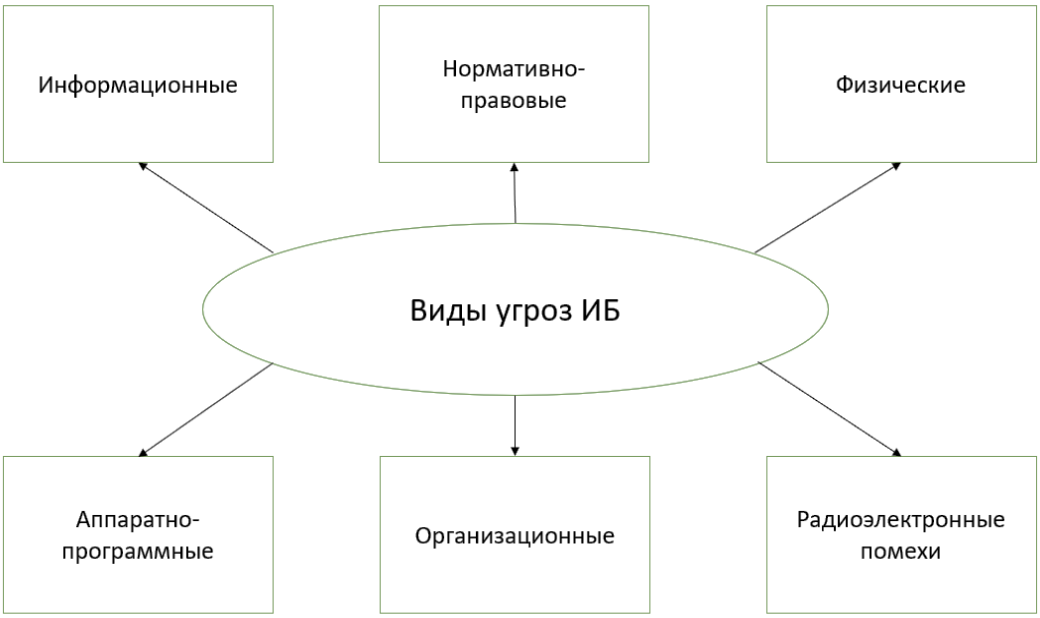

Рис. 1. Виды угроз ИБ

Информационные: преднамеренные и случайные ошибки при сборе и обработке данных, что может привести к утечкам и искажению информации. Аппаратно-программные: вирусы и устройства перехвата информации, такие как шпионские средства. Радиоэлектронные помехи: сбои в работе техники из-за внешних сигналов. Физические: уничтожение или поломка коммуникационных систем, похищение носителей информации. Организационные и нормативно-правовые: проблемы из-за устаревших технологий и недостатка нормативной базы[1].

Для обеспечения безопасности необходимо следовать множеству нормативных актов и инструкций, включая указания Федеральной службы по техническому и экспортному контролю.

В России основные объекты информационной безопасности можно классифицировать следующим образом.

1. Информационные ресурсы: данные с государственной тайной и конфиденциальной информацией.

2. Средства информатизации: программные средства, используемые для обработки данных.

3. Технические системы: системы, обрабатывающие открытую информацию, расположенные в помещениях с ограниченным доступом.

[1] Белов Б.А., Лось В.П. Основы информационной безопасности. М.: Горячая линия-Телеком, 2011. 558 с.

4. Помещения: места для закрытых переговоров и обсуждений сведений ограниченного доступа.

Что касается угроз информационной безопасности в государственных информационных и телекоммуникационных системах, выделяются следующие аспекты.

1. Внешние угрозы: деятельность иностранных спецслужб и преступных групп, нацеленная на несанкционированный доступ к информации.

2. Зависимость от импорта: использование импортных программно-аппаратных средств, что связано с отставанием отечественной промышленности.

3. Внутренние риски: нарушения регламентов обработки информации, ошибки персонала и сбои технических средств.

4. Некачественная защита: применение несертифицированных средств защиты информации.

5. Лицензирование: привлечение организаций без государственных лицензий для создания и защиты информационных систем.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Обеспечение защиты информации от перехвата и несанкционированного доступа
- Предотвращение утечек информации при использовании технических средств
- Защита информации от программно-технических воздействий разрушения и искажения
- Разработка современных требований при подключении к внешним сетям
- Обеспечение конфиденциальности в системах различного уровня защищенности
- Мониторинг появления устройств перехвата информации

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

- Лицензирование организаций в области защиты информации
- Аттестация объектов информатизации для соблюдения требований безопасности
- Сертификация средств защиты и контроль их эффективности
- Введение ограничений на использование защищаемых технических средств
- Создание защищенных информационных и автоматизированных систем управления

Безопасность данных требует их резервирования на разных носителях, что часто игнорируется. Специалисты должны помнить о необходимости распределения данных и защиты компьютеров от перепадов напряжения[1].

Организационные меры включают защиту носителей от кражи, подбор и обучение квалифицированного персонала, а также тестирование помещений на наличие шпионских устройств. Перед передачей информации важно правильно удалять конфиденциальные данные, так как файлы можно восстановить.

Для защиты от несанкционированного доступа используются системы идентификации и надежные пароли, которые необходимо регулярно менять. Эффективны также методы биометрической идентификации, такие как отпечатки пальцев и голосовые характеристики.

Криптография – ключевой метод защиты информации в телекоммуникациях, позволяющий зашифровывать сообщения. Для расшифровки требуется идентифицирующий ключ. Электронная цифровая подпись защищает официальные документы и широко используется в электронном документообороте[2].

Руководство предприятия должно разработать концепцию информационной безопасности и выделить средства на минимальный пакет защитных мер, включая антивирусное ПО, технологии аутентификации и шифрования данных.

Гришин А.Г.,

кандидат юридических наук
Ленинградский областной филиал
Санкт-Петербургского университета МВД России (п. Мурино)

Исследование методов обеспечения безопасности в сетях связи нового поколения

Развитие информационных технологий и повсеместное внедрение беспроводных сетей связи нового поколения ставят новые задачи по обеспечению их информационной безопасности. Уязвимости протоколов связи, сложность криптографических механизмов, большое число пользователей делают беспроводные сети привлекательной мишенью для злоумышленников.

Несанкционированный доступ к конфиденциальной информации, нарушение ее целостности и доступности могут привести к серьезным

[1] Биячуев Т.А. Безопасность корпоративных сетей. СПб: СПб ГУ ИТМО, 2004. 161 с.
[2] Конахович Г. Защита информации в телекоммуникационных системах. М.: МК-Пресс, 2005. 356 с.