ГЛАВА 3
Национальные стандарты по безопасности информационно-телекоммуникационных систем

— Скажите, пожалуйста, куда мне отсюда идти?

— А куда ты хочешь попасть? — ответил Кот.

— Мне все равно... — сказала Алиса.

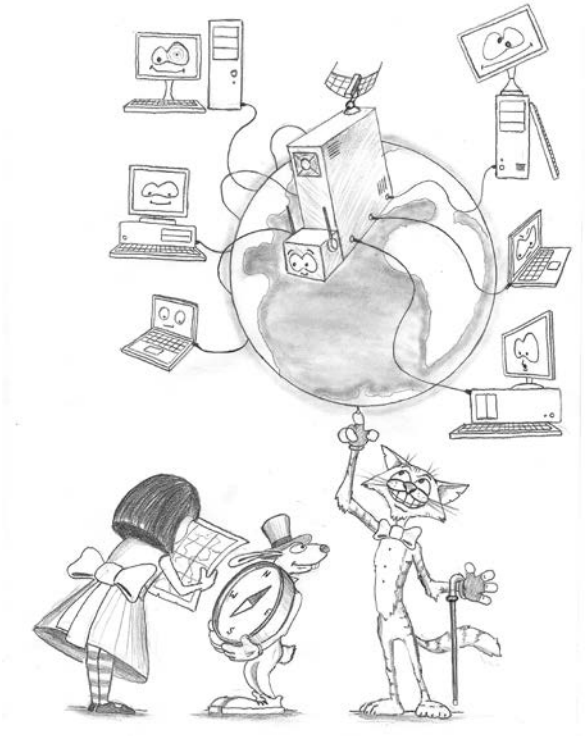
— Тогда все равно, куда и идти, — заметил Кот.

— ...только бы попасть куда-нибудь, — пояснила Алиса.

— Куда-нибудь ты обязательно попадешь, — сказал Кот. — Нужно только достаточно долго идти.

Не все ли равно, о чем спрашивать, если ответа все равно не получишь, правда?

Льюис Кэрролл. Алиса в Стране чудес



3.1. Список стандартов

К национальным стандартам в области защиты информации в автоматизированных (информационных) системах и сетях можно отнести следующие:

1. ГОСТ Р ИСО /МЭК 27033-1–2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».
2. ГОСТ Р ИСО /МЭК 27033-3–2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления».
3. ГОСТ Р 51583–2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
4. ГОСТ Р 56093–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства обнаружения преднамеренных силовых электромагнитных воздействий. Общие требования».
5. ГОСТ Р 56103–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения».
6. ГОСТ Р 52863–2007 «Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования».
7. ГОСТ Р 56115–2014 «Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования».
8. ГОСТ Р 53113.1–2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения».
9. ГОСТ Р 53113.2–2009 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов».
10. ГОСТ Р 53131–2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».
11. ГОСТ Р 56545–2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».
12. ГОСТ Р 56546–2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем».
13. ГОСТ Р 56824–2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет».
14. ГОСТ Р 53109–2008 «Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности».

15. ГОСТ Р 53110–2008 «Система обеспечения информационной безопасности. Сети связи общего пользования. Общие положения».
16. ГОСТ Р 53111–2008 «Устойчивость функционирования сети связи общего пользования. Требования и методы проверки».
17. ГОСТ Р 52448–2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения».
18. ГОСТ Р 56938–2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения».
19. ГОСТ Р 56205–2014 IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели».
20. ГОСТ Р МЭК 62443-2-1–2015 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики».
21. ГОСТ Р 56498–2015 (IEC/PAS 62443-3:2008) «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления».
22. ГОСТ Р МЭК 62443-3-3–2016 «Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности».
23. ГОСТ Р ИСО/МЭК 30100-1–2017 «Информационные технологии (ИТ). Менеджмент ресурсов домашних сетей. Часть 1. Требования».
24. ПНСТ 199–2017 «Глобальная навигационная спутниковая система. Региональные навигационно-информационные системы. Назначение, состав и характеристики системы обеспечения информационной безопасности».
25. ГОСТ Р 58256–2018 «Защита информации. Управление потоками информации в информационной системе. Формат классификационных меток».

Кроме указанных стандартов, в данной главе рассмотрены еще стандарты по защите прав на объекты интеллектуальной собственности:

ГОСТ Р 58086–2018 «Интеллектуальная собственность. Распределение интеллектуальных прав между заказчиком, исполнителем и автором на охраняемые результаты интеллектуальной деятельности, создаваемые и/или используемые при выполнении научно-исследовательских, опытно-конструкторских, технологических и производственных работ».

ГОСТ Р 56823–2015 «Интеллектуальная собственность. Служебные результаты интеллектуальной деятельности».

ГОСТ Р 55386–2012 «Интеллектуальная собственность. Термины и определения (с Изменением № 1)».

ГОСТ Р 58210–2018 «Информационные технологии. Сети будущего. Формулировка проблем и требования. Часть 1. Общие аспекты».

ПНСТ 301–2018/ИСО/МЭК 24767-1:2008 «Информационные технологии. Безопасность домашней сети. Часть 1. Требования безопасности».

ГОСТ Р ИСО/МЭК 24767-2–2018 «Информационные технологии. Безопасность домашней сети. Часть 2. Внутренние службы безопасности. Безопасный протокол связи для связующего программного обеспечения (SCPM)».

3.2. Стандарты серии 27033 по безопасности сетей

3.2.1. Общие замечания

В современном мире информационные системы большинства организаций связаны сетями, при этом сетевые соединения могут относиться к одному или нескольким видам, представленным на рис. 3.1 (как они изображены в стандарте ГОСТ Р ИСО/МЭК 27033-1–2011):

- в пределах организации;
- между различными организациями;
- между организацией и неограниченным кругом лиц.

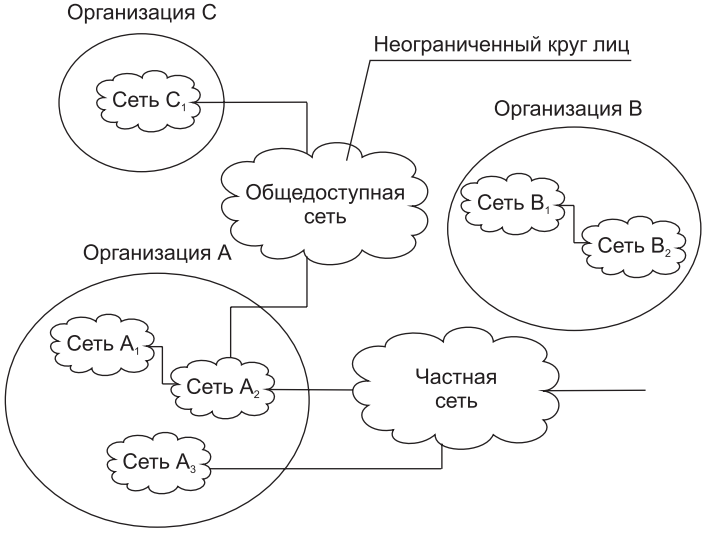


Рис. 3.1. Виды сетевых соединений

Использование сетевых технологий, в том числе глобальной информационно-телекоммуникационной сети Интернет, обеспечивает новые широкие возможности для ведения бизнеса и получения значительных преимуществ. Однако наряду с преимуществами появляются новые риски безопасности, которые могут оказывать существенное неблагоприятное влияние на деятельность организации, а следовательно, требуют управления. Поэтому одним из важнейших требований при использовании сетевых технологий является обеспечение адекватной защиты сетей, информационных систем, сетевых сервисов и обрабатываемой информации.

Назначение стандартов серии ИСО/МЭК 27033 состоит в том, чтобы предоставить подробные рекомендации по аспектам безопасности менеджмента, функционирования и использования сетей и информационных систем. Они предоставляют дополнительные