

VII МЕЖДУНАРОДНЫЙ ФОРУМ БЕЗОПАСНОГО ИНТЕРНЕТА – ФБИ-2016
27.04.2016, МОСКВА, ЗУБОВСКИЙ Б-Р, 4, МИА «РОССИЯ СЕГОДНЯ»

МЕТОДЫ СИСТЕМНОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРЫ СВЯЗИ

Ефимушкин В.А.

заместитель генерального директора
по научной работе ФГУП ЦНИИС,
к.ф.-м.н., доцент, член Президиума МАС

Результаты поиска по запросам «Информационная безопасность» и «телекоммуникации»

Поисковая последовательность	yandex найденных ответов, млн.
Информационная безопасность	56
Телекоммуникации	3

Пока во многих случаях обеспечение безопасности инфраструктуры связи (БИС) сводится к противостоянию конкретным угрозам, а не к принятию общей стратегии обеспечения безопасности, основанной на оценке рисков.

Под ИБ инфокоммуникационных сетей следует понимать организационно-техническую систему обеспечения защищённости сбалансированных интересов потребителей, операторов и органов государственной власти в информационной сфере сети.

В свою очередь информационная сфера представляет собой совокупность информации, информационной инфраструктуры, включая инфраструктуру связи, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования отношений, возникающих при использовании инфокоммуникационных сетей.

Инфраструктура связи как объект защиты является сложной системой с наличием обратных связей, взаимодействием с другими системами, возникновением новых неожиданных свойств объекта в процессе его эксплуатации и др.

Основные задачи обеспечения БИС

- **Обеспечение физической безопасности оборудования**
- **Создание доказательной базы для привлечения нарушителей к ответственности**
- **Противодействие распространению вредоносных программ и спама**
- **Обеспечение контроля функционирования**
- **Защиту информации управления сетью и информации потребителей**
- **Обеспечение защищённости сбалансированных интересов потребителей, операторов и регулирующих органов**
- **Борьба с мошенничеством**
- **Обеспечение приватности**

Проблема БИС подразделяется на классы:

- ИБ подсистем**
- сетевая безопасность**
- ситуационная безопасность**
- техническая безопасность**

Управление БИС является важнейшей задачей, особенно актуальной для крупных сетей.

Система управления должна интегрировать в себе возможности настройки, отладки и мониторинга межсетевых экранов, VPN устройств, систем обнаружения вторжений, позволять простую реализацию и поддержку систем безопасности.

Обеспечение БИС включает две группы задач:

- обеспечение безопасности на стадии проектных и строительных работ**
- обеспечение безопасности на стадии эксплуатации**

Под проектно-строительной БИС подразумеваются требования по обеспечению защищённости сетей, систем, служб связи от угроз БИС на стадии разработки, строительства и сдачи в эксплуатацию объектов сети.

Под эксплуатационной БИС понимается состояние защищённости сетей, систем, служб связи от несанкционированных или непреднамеренных воздействий нарушителя, способных ухудшить эксплуатационные характеристики сетей, систем в процессе их функционирования.

Все мероприятия по обеспечению БИС не должны ухудшать качественных характеристик сети и снижать оперативность её работы.

Программы подготовки специалистов высшей школы

- Организация и технология защиты информации № 075300
- Комплексная защита объектов информатизации № 075400
- Информационная безопасность телекоммуникационных систем № 075600
- Защищенные системы связи
- Комплексное обеспечение информационной безопасности автоматизированных систем № 075500
- Компьютерная безопасность № 075200

- Анализ рисков и оборонительные модели
- Разработка политики безопасности
- Организация безопасности
- Контроль доступа: физическая безопасность, аутентификация и контроль авторизации, архитектура безопасности данных, архитектура управления безопасностью
- Архитектура безопасности: структура сети, безопасность сетевого оборудования, межсетевые экраны, безопасность виртуальных частных сетей, безопасность беспроводных сетей, системы обнаружения вторжений, архитектура целостности и доступности, ролевой принцип организации безопасности сетей
- Безопасность операционной системы
- Безопасность приложений
- Аварийное восстановление и обеспечение бесперебойной деятельности
- Атаки и противодействие им
- Реагирование на инциденты и судебная экспертиза
- Проблемы законодательства: законы, имеющие отношение к деятельности специалистов по информационной безопасности

Спасибо за внимание!



Ефимушкин Владимир Александрович ef@zniis.ru (985) 215-17-75