

Министерство образования Республики Беларусь  
Учреждение образования  
«Белорусский государственный университет  
информатики и радиозлектроники»

Факультет инфокоммуникаций

Кафедра инфокоммуникационных технологий

**М. Н. Бобов, О. Г. Шевчук**

## ***ЗАЩИТА ИНФОРМАЦИИ В СЕТЯХ ИНФОКОММУНИКАЦИЙ***

*Рекомендовано УМО по образованию в области информатики  
и радиозлектроники в качестве учебно-методического пособия для  
специальности 1-45 80 01 «Системы и сети инфокоммуникаций»*

Минск БГУИР 2021

## Содержание

Введение.....	4
1 Описание структуры защищенной локально-вычислительной сети.....	5
1.1 Зона подключения к глобальной сети.....	5
1.2 Зона управления безопасностью и ресурсами сети.....	6
1.3 Зона защищаемых данных, обрабатываемых в ЛВС.....	6
2 Аутентификация.....	7
2.1 Локальная аутентификация.....	7
2.2 Удаленная аутентификация.....	14
2.3 Протоколы защищенных сокетов.....	17
2.4 Протокол обеспечения безопасности IpSec в сети Интернет.....	19
2.5 Протоколы управления ключами.....	23
3 Механизмы управления доступом к информации.....	26
3.1 Управление доступом по ключам (мандатная система доступа).....	26
3.2 Управление доступом по спискам.....	27
3.3 Управление доступом на основе матриц.....	29
3.4 Управление доступом по уровням секретности.....	30
4 Криптографическая защита информации.....	32
4.1 Основы криптографической защиты информации.....	32
4.2 Стандарты симметричных систем шифрования.....	34
4.3 Асимметричные криптосистемы.....	45
5 Механизмы электронной цифровой подписи.....	50
5.1 СТБ 34.101.45-2013. Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых.....	50
5.2 СТБ 1176.2-99. Процедуры выработки и проверки электронной цифровой подписи.....	54
6 Контроль целостности.....	57
6.1 Имитозащита сообщений в ИКС.....	57
6.2 Контроль целостности сообщений на основе функций хэширования...	61
Список использованных источников.....	67