Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 7

Криптографические методы защиты информации (КМЗИ)

Толстой Александр Иванович

к.т.н., доцент

Доцент кафедры «Информационная безопасность банковских систем»

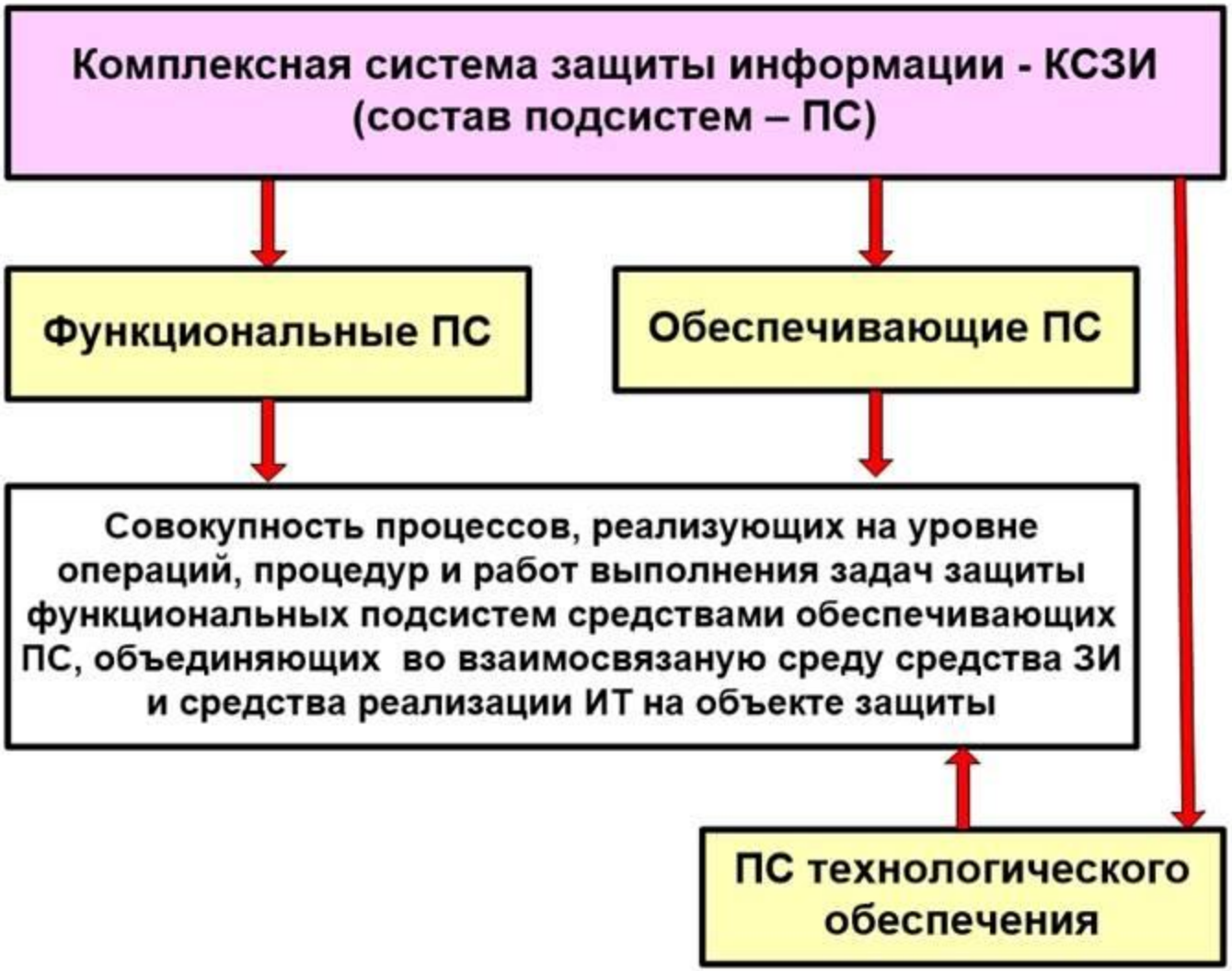
НИЯУ МИФИ,

Факультет «Кибернетика и информационная безопасность»,

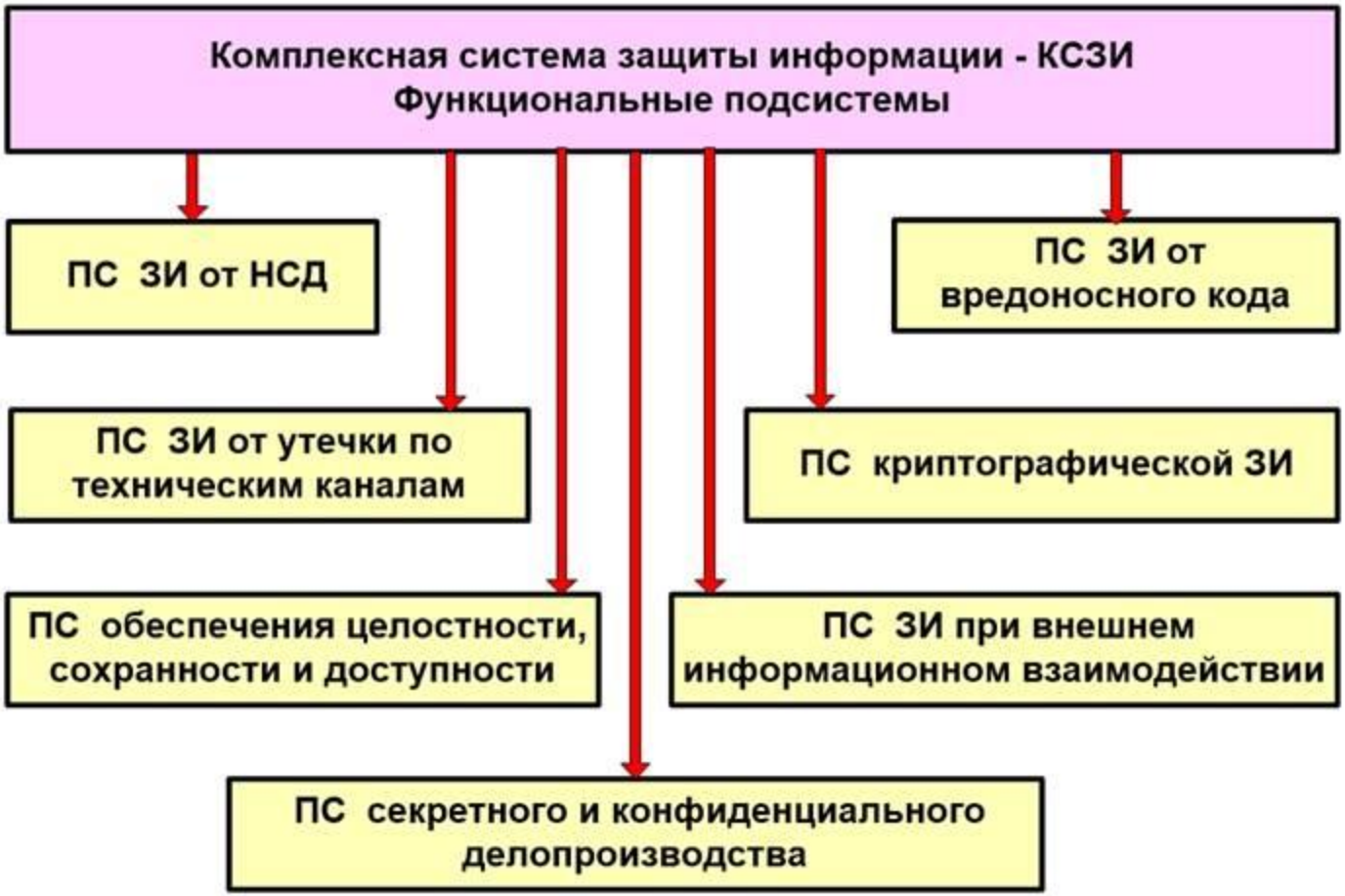
кафедра

Москва, 2017

***«Комплексная система защиты информации» (КСЗИ)*- совокупность различных подсистем.**



***«Комплексная система защиты информации» (КСЗИ)*- совокупность различных подсистем.**



ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

10.8.1 Политики и процедуры обмена информацией

Должны существовать формальные политики, процедуры и меры и средства контроля и управления в отношении обмена информацией с целью защиты такого обмена, когда используются все типы средств связи.

Процедуры, меры и средства контроля и управления, которые необходимо соблюдать при использовании электронных средств связи для обмена информацией, должны учитывать следующее:

……

g) использование криптографических методов, например для защиты конфиденциальности, целостности и аутентичности информации (см. 12.3);

ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

12.3 Криптографические меры и средства контроля и управления

Цель: Защищать конфиденциальность, аутентичность или целостность информации, используя криптографические средства.

Необходимо разработать политику в отношении использования криптографических мер и средств контроля и управления. Для поддержки использования криптографических методов следует применять управление ключами.

ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».

Криптографические меры и средства контроля и управления могут использоваться для достижения различных целей безопасности, например:

a) конфиденциальности посредством использования шифрования информации для защиты чувствительной или критической информации как хранимой, так и передаваемой;

b) целостности/аутентичности посредством использования цифровых подписей или кодов аутентификации сообщений для защиты аутентичности и целостности, хранимой или передаваемой чувствительной или критической информации;

c) неотказуемости, посредством использования криптографических методов для получения подтверждения того, что событие или действие имело или не имело место.

1.Введение в информационную безопасность: Учебное пособие для вузов/ А.А.Малюк, В.С.Горбатов, В.И.Королев и др.; Под ред. В.С.Горбатова . – М.: Горячая линия–Телеком, 2011.

Стр. 100-146

Глава четвертая

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

2.Дисциплина: «Основы криптографической защиты информации»

1-ый семестр

Благодарю за внимание!

Толстой Александр Иванович

AlTolstoj@mephi.ru