



Основы информационной безопасности критически важных объектов

**Учебная дисциплина ОИБ КВО
Темы 3, ..., 10**

Толстой Александр Иванович

К.Т.Н., доцент

**Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ**



Москва, 2017



Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 3

Нормативно-правовое обеспечение

Толстой Александр Иванович

К.Т.Н., доцент

**Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ**



Москва, 2017

3. Нормативно-правовое обеспечение



3.1. Предмет и содержание проблемы

3.2. Нормативно правовая база ИБ в РФ

3.3. Техническое регулирование в области ИБ

3.4. Стандартизация обеспечения ИБ

3.5. Нормативно-правовое обеспечение безопасности КВО



Основы информационной безопасности критически важных объектов

**Учебная дисциплина ОИБ КВО
Тема 4**

Исходная концептуальная схема обеспечения ИБ

Толстой Александр Иванович

К.Т.Н., доцент

Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ



Москва, 2017

4.Исходная концептуальная схема обеспечения ИБ

4.1.Традиционный подход

4.2.Специфика обеспечения ИБ

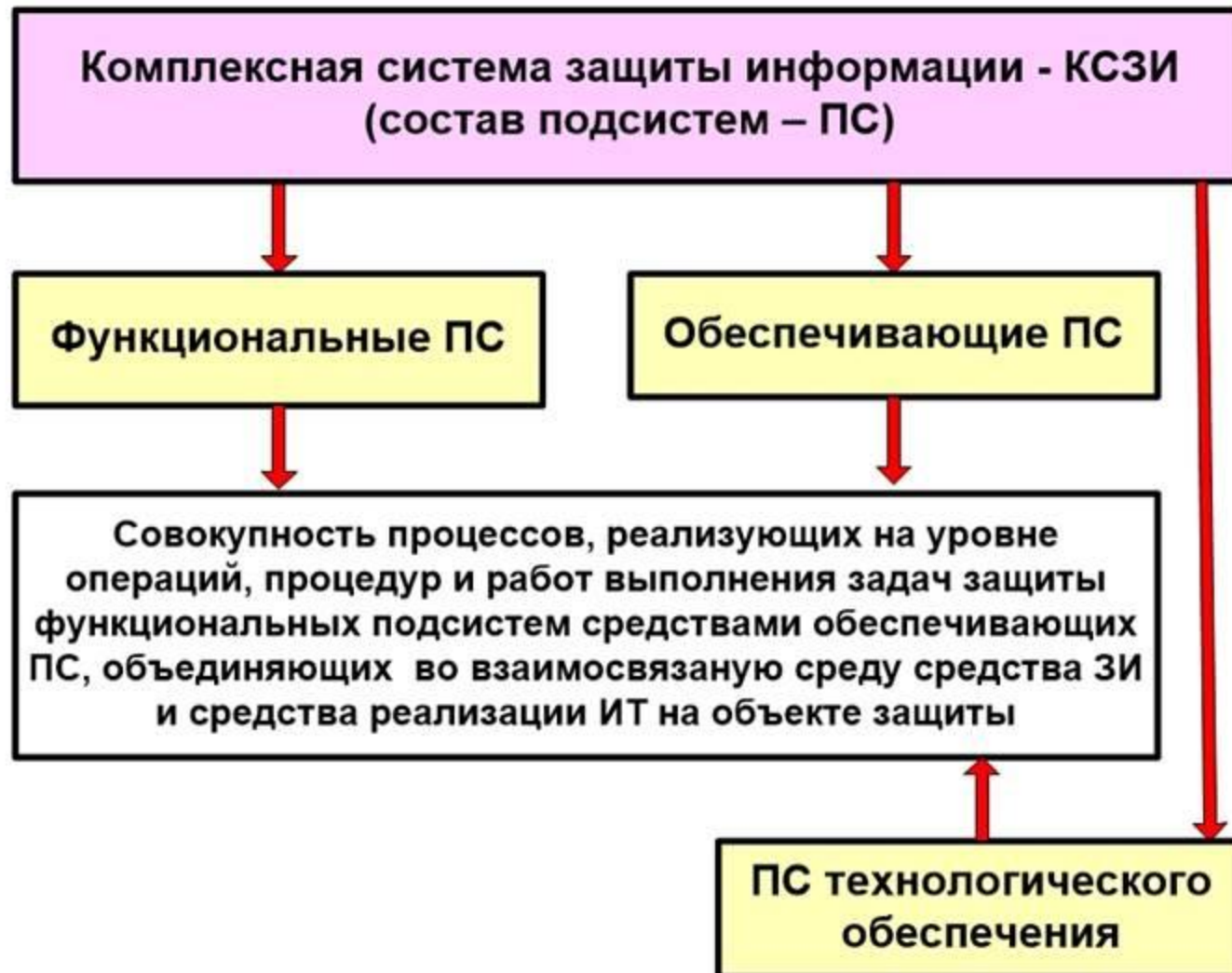
4.3.Современный подход к обеспечению ИБ

4.4.Система управления ИБ



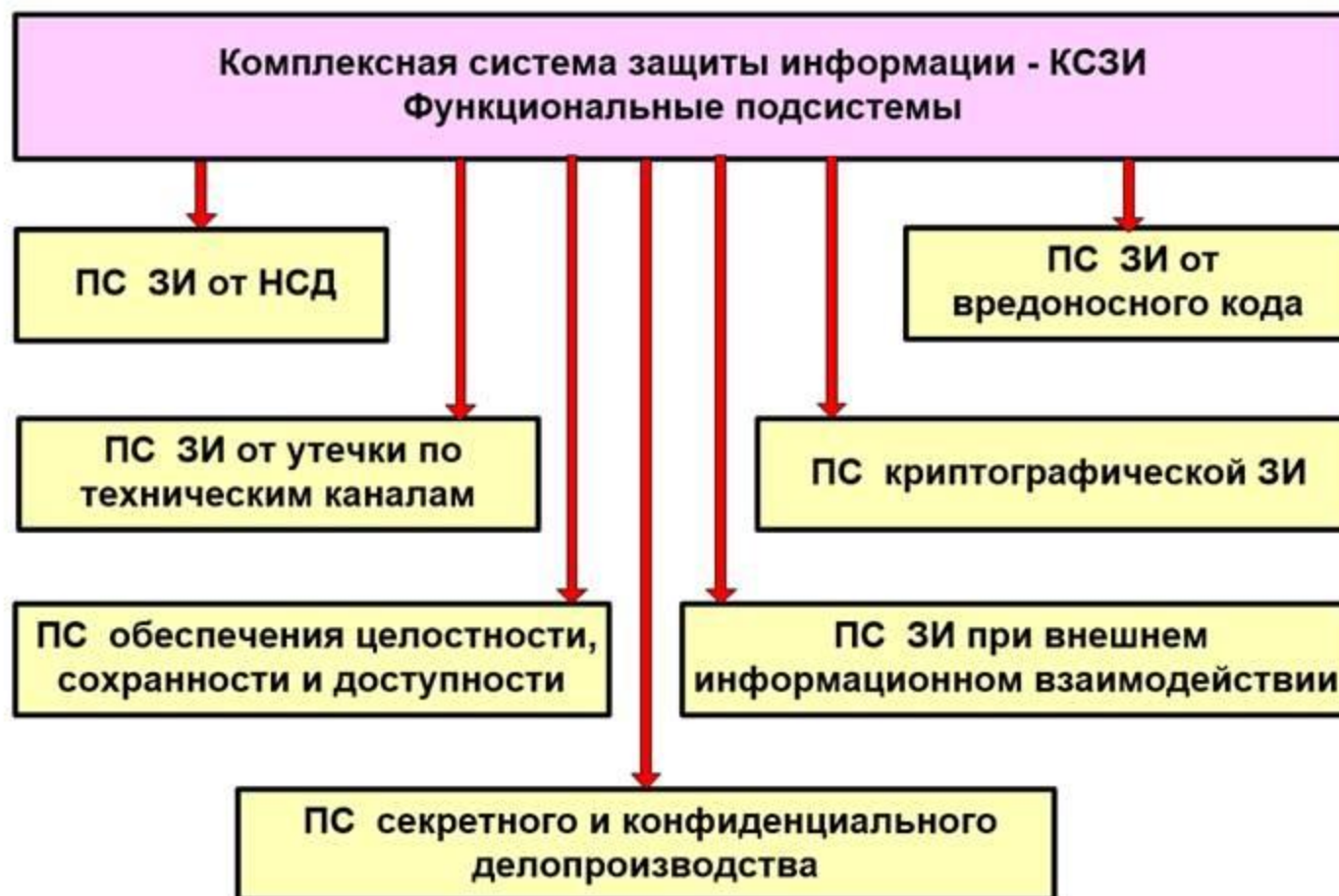
4.1. Традиционный подход

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



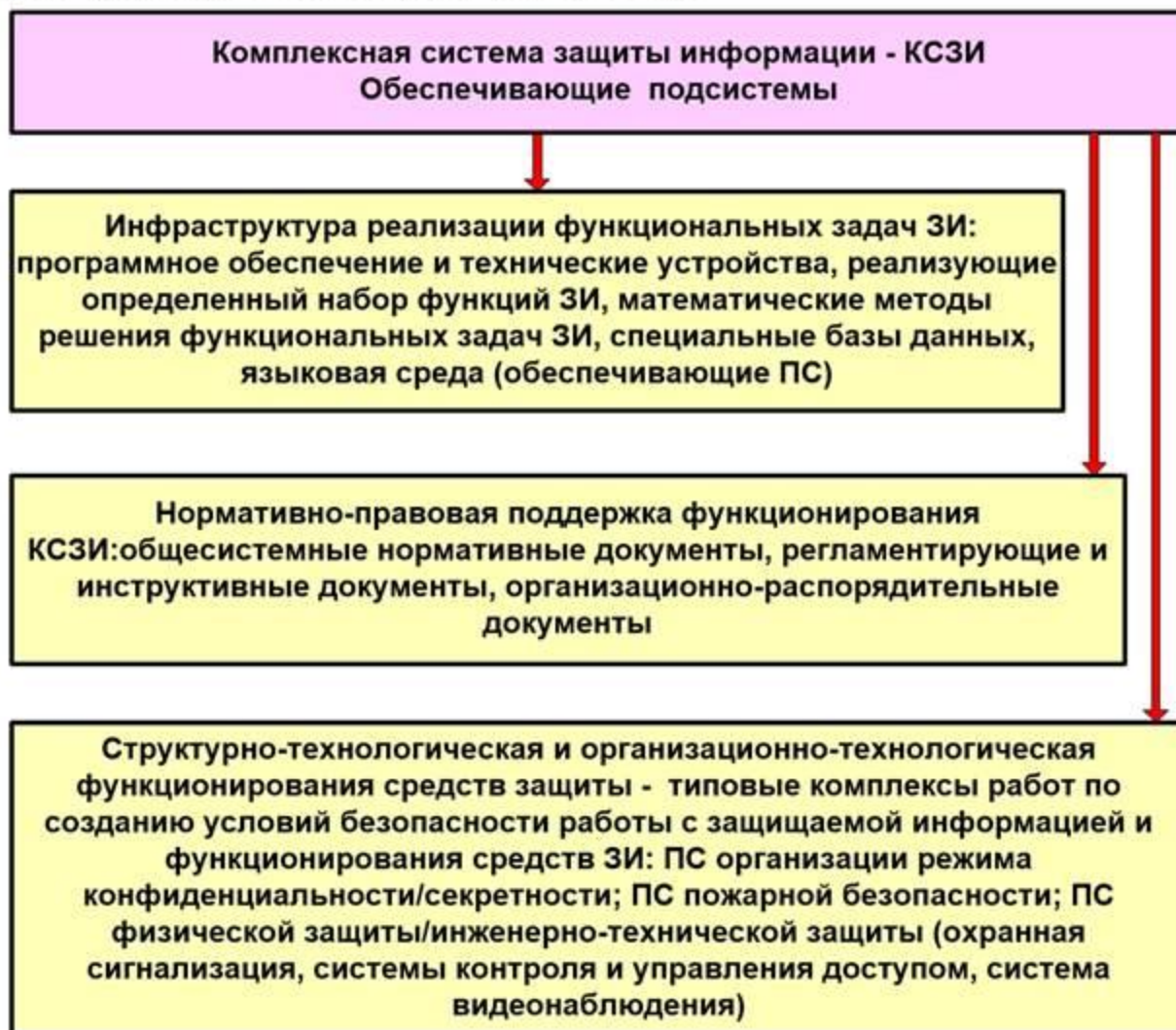
4.1. Традиционный подход

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



4.1. Традиционный подход

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



4.3.Современный подход к обеспечению ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ **Эффективность обеспечения ИБ определяется эффективностью управления**
- ✓ **Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.**
- ✓ **Активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе.**
- ✓ **Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.**
- ✓ **Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ.**
- ✓ **Управление инцидентами ИБ является элементом управления ИБ.**
- ✓ **Контроль обеспечения ИБ является элементом управления ИБ**

4.4. Система управления ИБ

Основные идеи новой концептуальной схемы обеспечения ИБ:

- ✓ Эффективность обеспечения ИБ определяется эффективностью управления
- ✓ Основной целью деятельности службы ИБ организации является содействие бизнесу – целям деятельности организации.
- ✓ Активы могут рассматриваться только в контексте целей деятельности организации, но не как иначе.
- ✓ Деятельности организации сопутствует значительное число различных рисков – риски ИБ один из видов рисков.
- ✓ Менеджмент рисков ИБ – основа деятельности по обеспечению ИБ.
- ✓ Управление инцидентами ИБ является элементом управления ИБ.
- ✓ Контроль обеспечения ИБ является элементом управления ИБ:

Основные процессы управления ИБ:

1. Управление рисками ИБ.

2. Управление инцидентами ИБ.

3. Проверка и оценка деятельности по управлению ИБ

4. Взаимодействие с управлением непрерывностью бизнеса

4.4. Система управления ИБ

Работа с процессами СУИБ: Основные процессы СУИБ





Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 5

Защита информации от несанкционированного доступа (НДС) (ЗИотНДС)

Толстой Александр Иванович

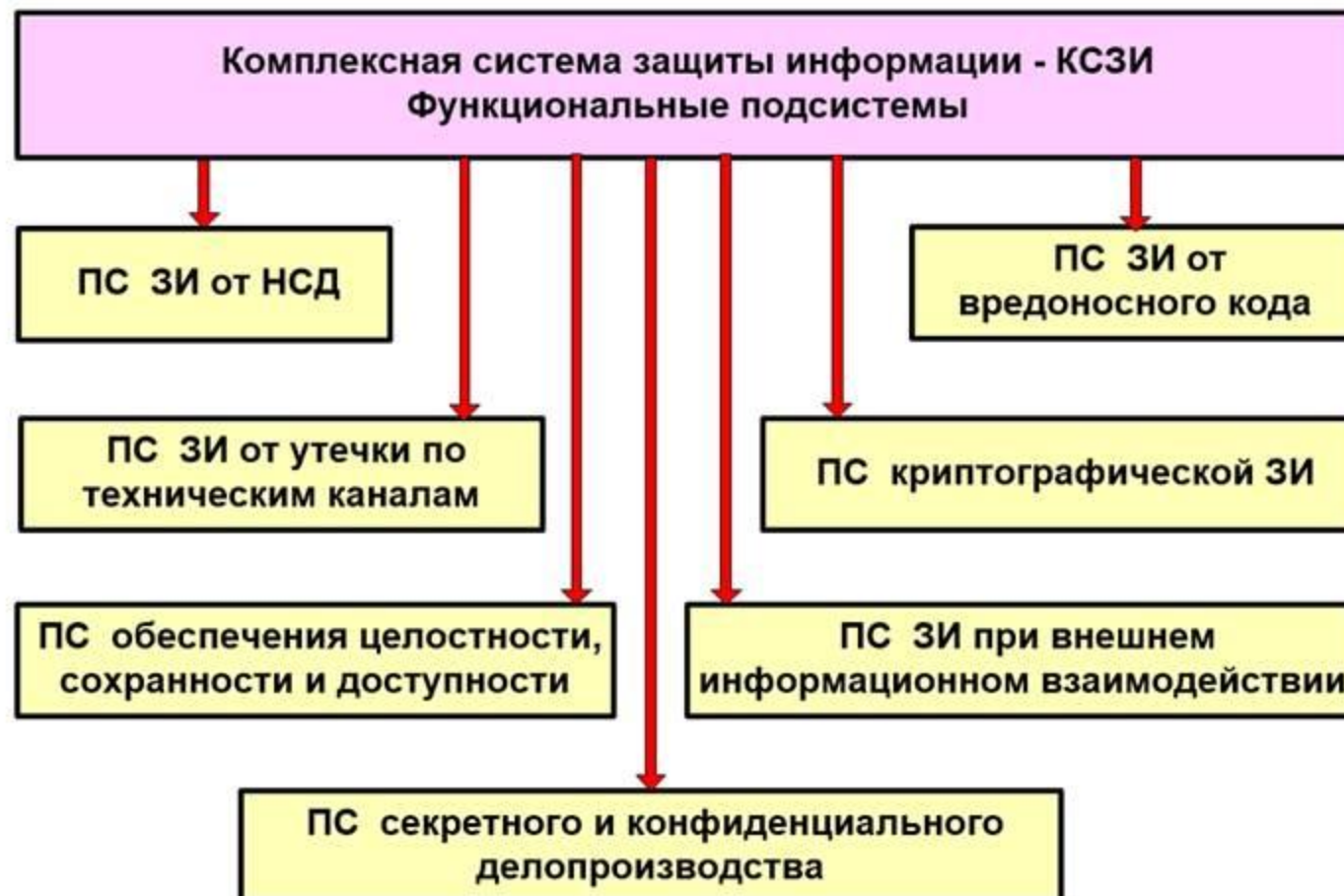
К.Т.Н., доцент

**Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ**



Москва, 2017

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



Содержание



1. Введение

2. Основные модели защиты

3. Авторизация субъектов доступа

4. Основные способы НСД

5. Основы ЗИ от НСД

6. Категорирование информации

7. Управление доступом в АС

8. Обзор программно-аппаратных средств ЗИ от НСД

9. Основные навыки ЗИ от НСД



Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 6

Защита информации от воздействий вредоносных программ (ЗотВП)

Толстой Александр Иванович

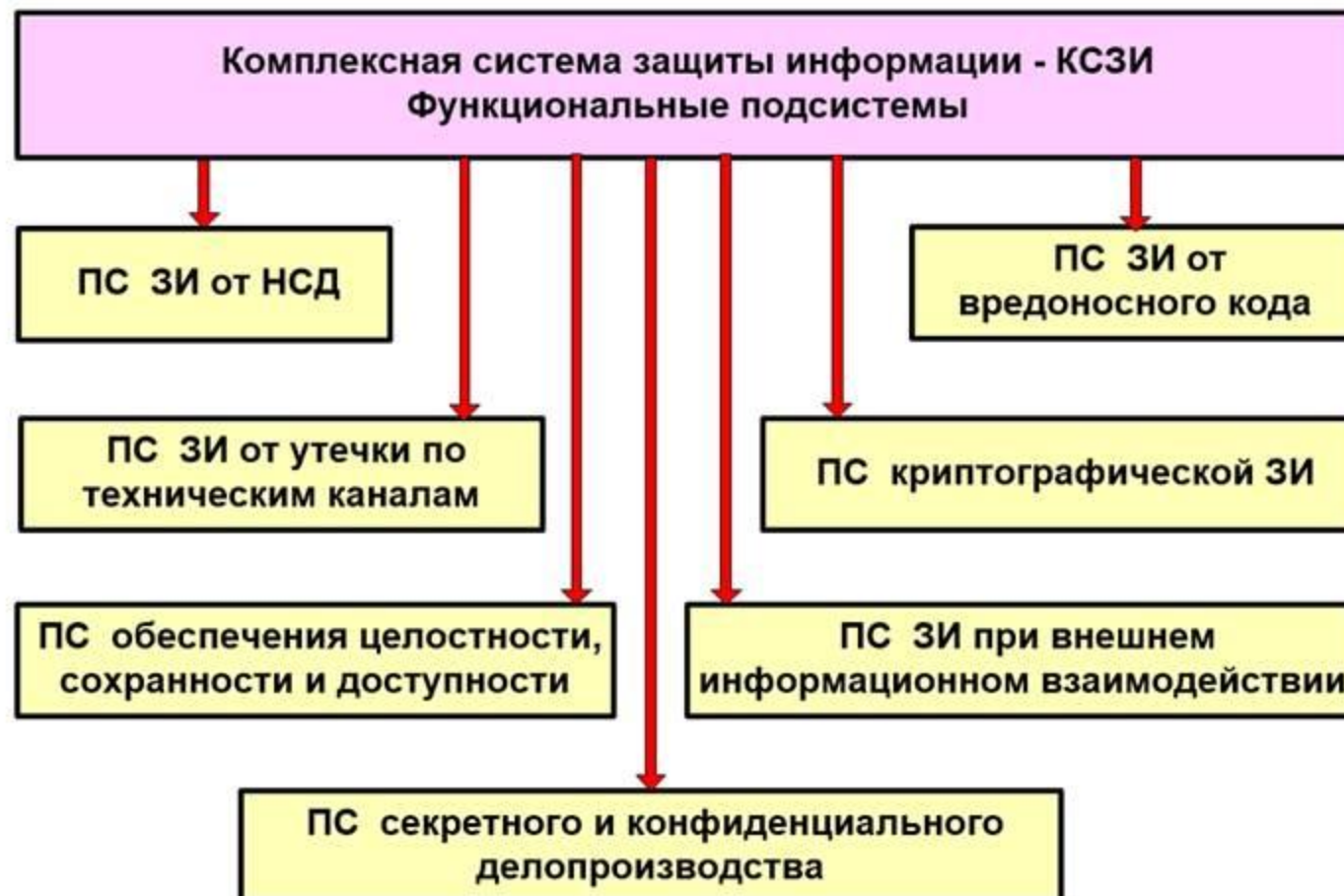
К.Т.Н., доцент

**Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ**



Москва, 2017

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



Содержание

1. Введение

2. Основные понятия и виды вредоносных программ (ВП)

3. Способы защиты от воздействия ВП

4. Основные виды антивирусных средств

5. Общие требования по обеспечению ИБ от воздействия ВП

6. Основные навыки антивирусной защиты





Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 7

Криптографические методы защиты информации (КМЗИ)

Толстой Александр Иванович

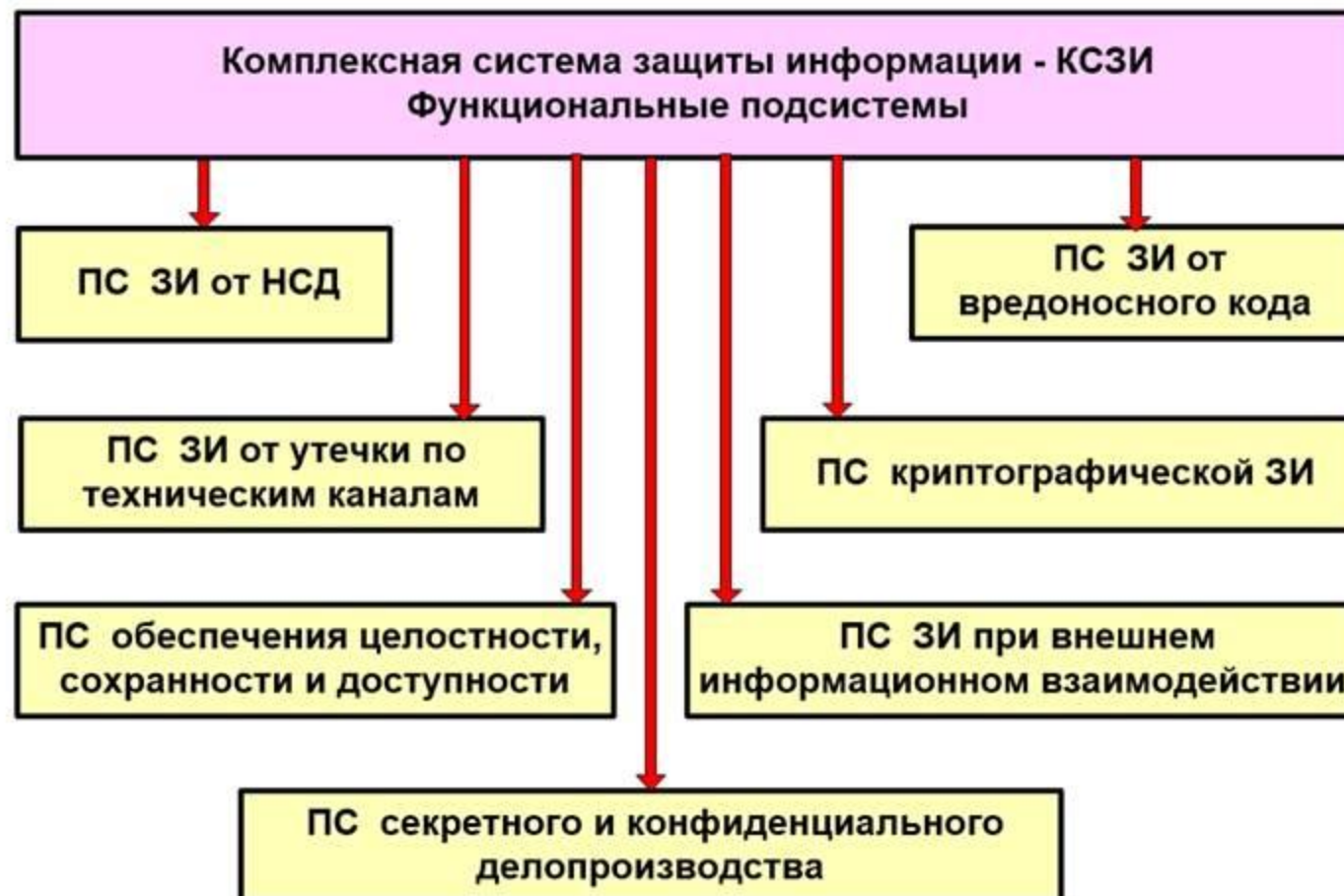
К.Т.Н., доцент

**Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ**



Москва, 2017

«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:

- а) конфиденциальности посредством использования шифрования информации для защиты чувствительной или критической информации как хранимой, так и передаваемой;
- б) целостности/аутентичности посредством использования цифровых подписей или кодов аутентификации сообщений для защиты аутентичности и целостности, хранимой или передаваемой чувствительной или критической информации;
- с) неотказуемости, посредством использования криптографических методов для получения подтверждения того, что событие или действие имело или не имело место.

**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**



Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 8

Защита информации от утечки по техническим каналам (ЗИ ТКУ)

Толстой Александр Иванович

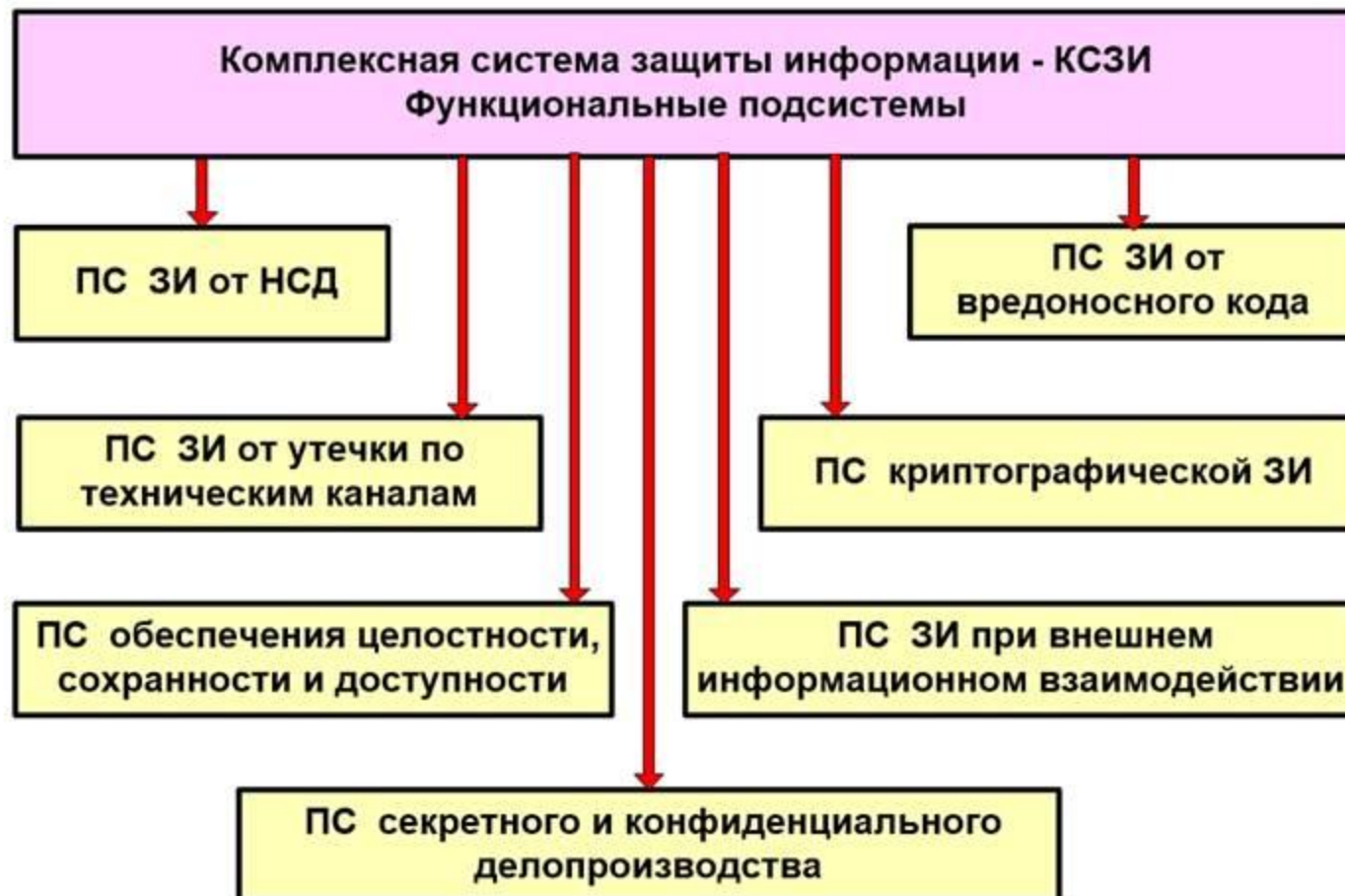
К.Т.Н., доцент

**Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ**



Москва, 2017

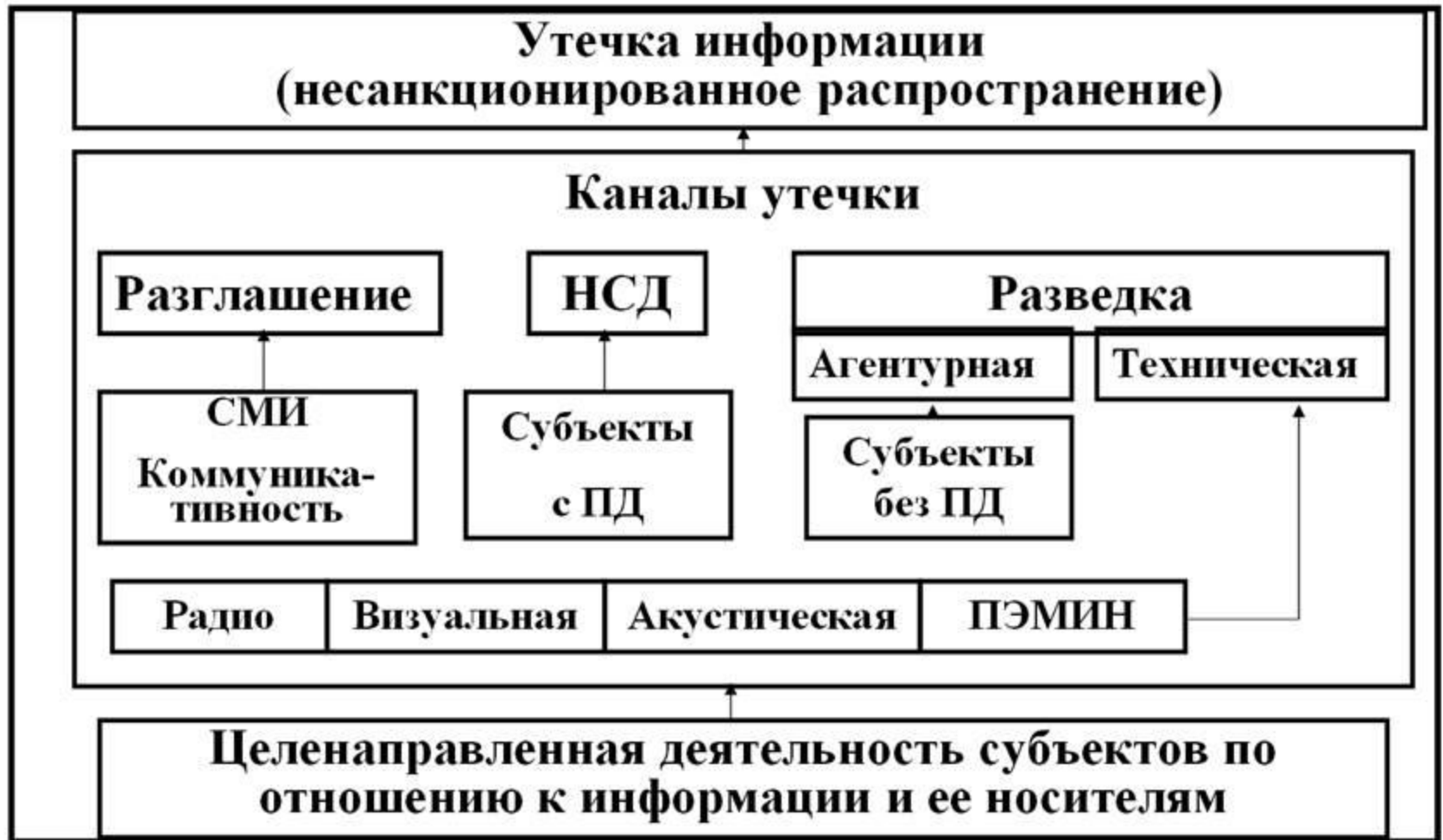
«Комплексная система защиты информации» (КСЗИ) - совокупность различных подсистем.



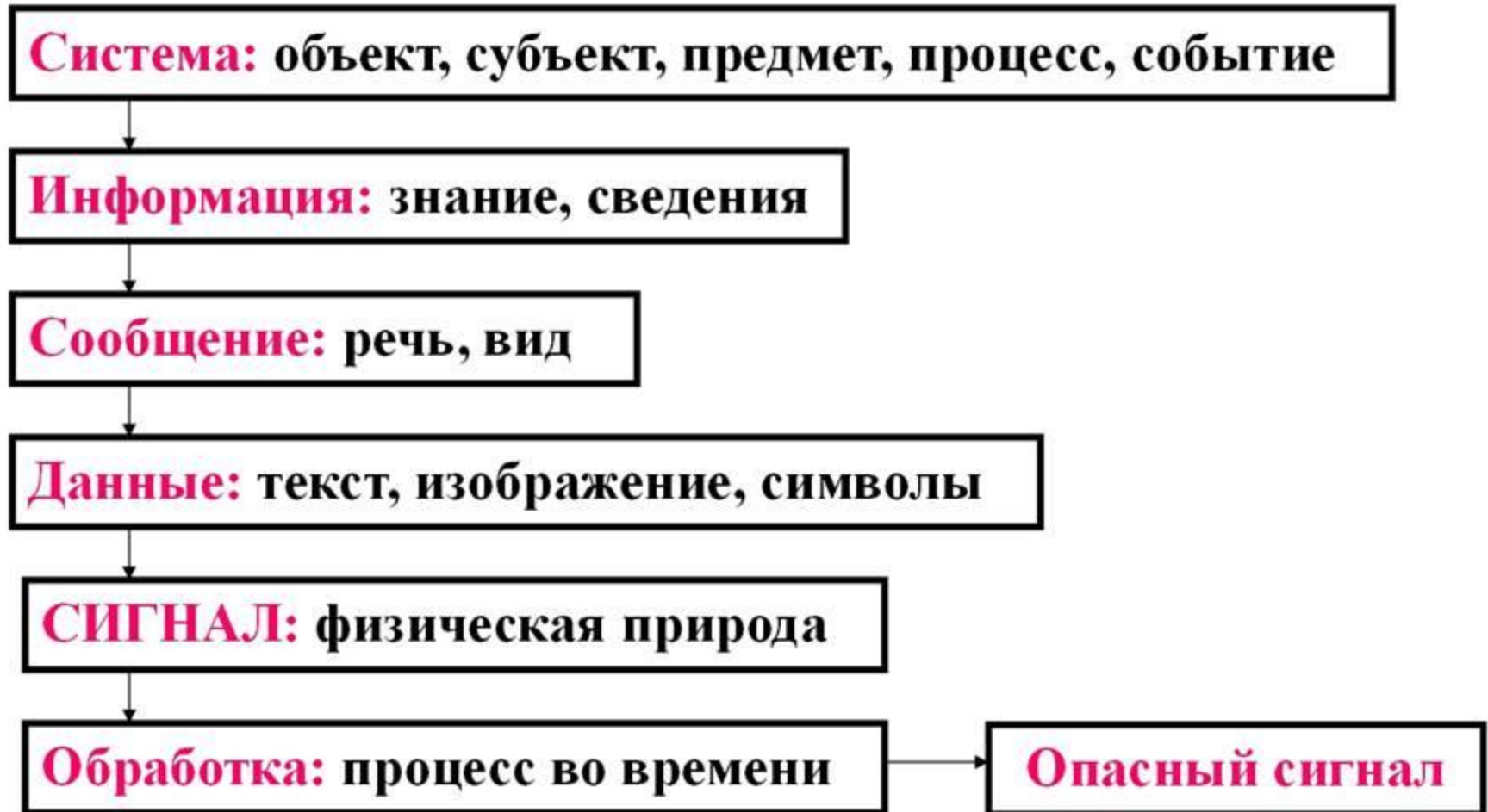
При обработке информации на технических средствах всегда происходит ее утечка по техническим каналам, но не всегда это приводит к опасным последствиям

Технический канал утечки информации (ТКУИ) ?

Технический канал утечки информации (ТКУИ) ?



Технический канал утечки информации (ТКУИ) ?

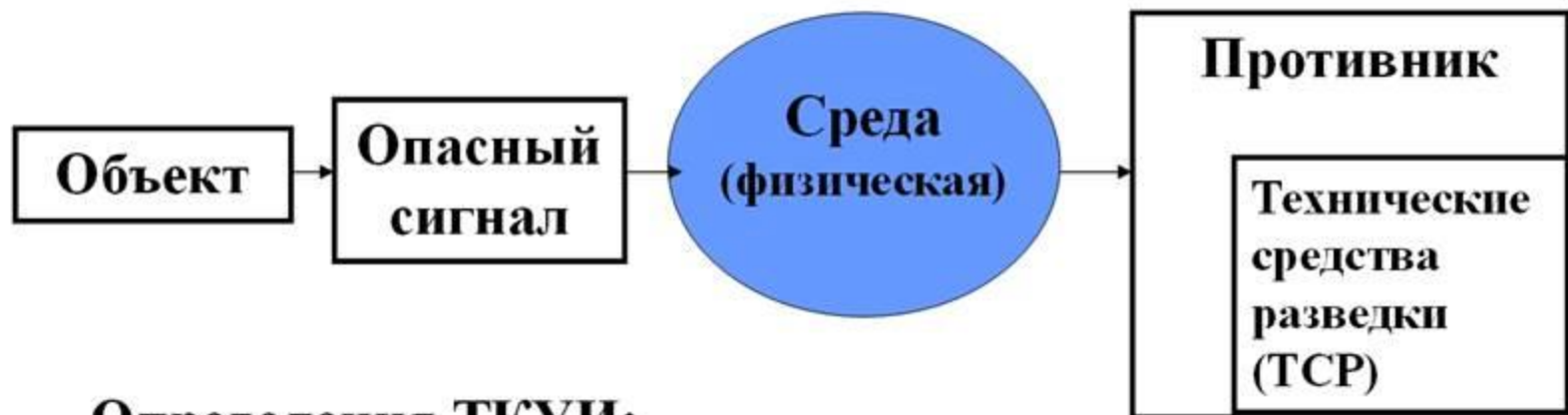


Технический канал утечки информации (ТКУИ) ?



Технический канал утечки информации (ТКУИ) ?

Технический канал утечки информации (ТКУИ)



Определения ТКУИ:

1. $\text{ТКУИ} = \text{Объект} + \text{ТСР} + \text{Среда}$
2. $\text{ТКУИ} = \text{Физические поля (среда)} + \text{Элементы конструкции объекта} + \text{ТСР}$

8.2. Технические каналы утечки информации (ТКУИ)

Основа классификации ТКУИ:



- **Классификация сообщений** (текст, речь, изображение, данные)
- **Классификация сигналов** (визуально-оптический, акустический, электрический, электромагнитный)
- **Классификация источников опасных сигналов** (документы: текстовые, графические; объект в целом; человек: его речь; технические средства обработки информации: ТСО основные и ТСО вспомогательные)
- **Классификация способов НСД к информации** (подслушивание, перехват, незаконное подключение, копирование, подделка, наблюдение, фотографирование, видеозапись, хищение)

8.2. Технические каналы утечки информации (ТКУИ): классификация ТКУИ

Объект	Сообщение	Опасный сигнал	Способ НСД	Вид ТКУИ
Док-ты «ТВ»	Текст	Материально-вещественный	Хищение, копирование, подделка, фотографирование, видеозапись	Материально-вещественный
Док-ты «ЭВ»	Данные	Материально-вещественный	Хищение, копирование, подделка,	Материально-вещественный
Человек	Речь	Акустический	Подслушивание	Акустический
Объект в целом	Вид	Визуально-оптический	Наблюдение, фотографирование, видеозапись	Визуально-оптический
ТСОИ, ВТС	Данные	Электрический Электромагнитный	Перехват, незаконное подключение	Электрический, Электромагнитный
Каналы связи	Данные	Электрический Электромагнитный	Перехват, незаконное подключение	Электрический, Электромагнитный
СЗУ	Данные	Электрический Электромагнитный, оптический	Перехват, незаконное подключение, аудио, видеозапись	Электрический, Электромагнитный

8.2. Технические каналы утечки информации (ТКУИ): классификация ТКУИ

Способ НСД	Технический канал утечки информации			
	Электрический Электромагнитный	Акусти- ческий	Визуально- оптический	Материально- вещественный
Подслушивание	+	+		
Копирование	+			+
Подделка	+			+
Перехват	+	+		
Незаконное подключение	+	+		
Наблюдение			+	
Фотографи- рование, видеозапись			+	
Хищение				+

**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. 147-175

Глава пятая

ПРОТИВОДЕЙСТВИЕ УТЕЧКЕ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 9

Информационная безопасность автоматизированных систем критически важных объектов (ИБ АСУ КВО)



Толстой Александр Иванович

К.Т.Н., доцент

**Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ**



Москва, 2017

Содержание

9.1. Введение

9.2. Структура АСУ ТП

9.3. Обеспечение ИБ в АСУ ТП

9.4. Объекты защиты в АСУ ТП

9.5. Угрозы ИБ для АСУ ТП

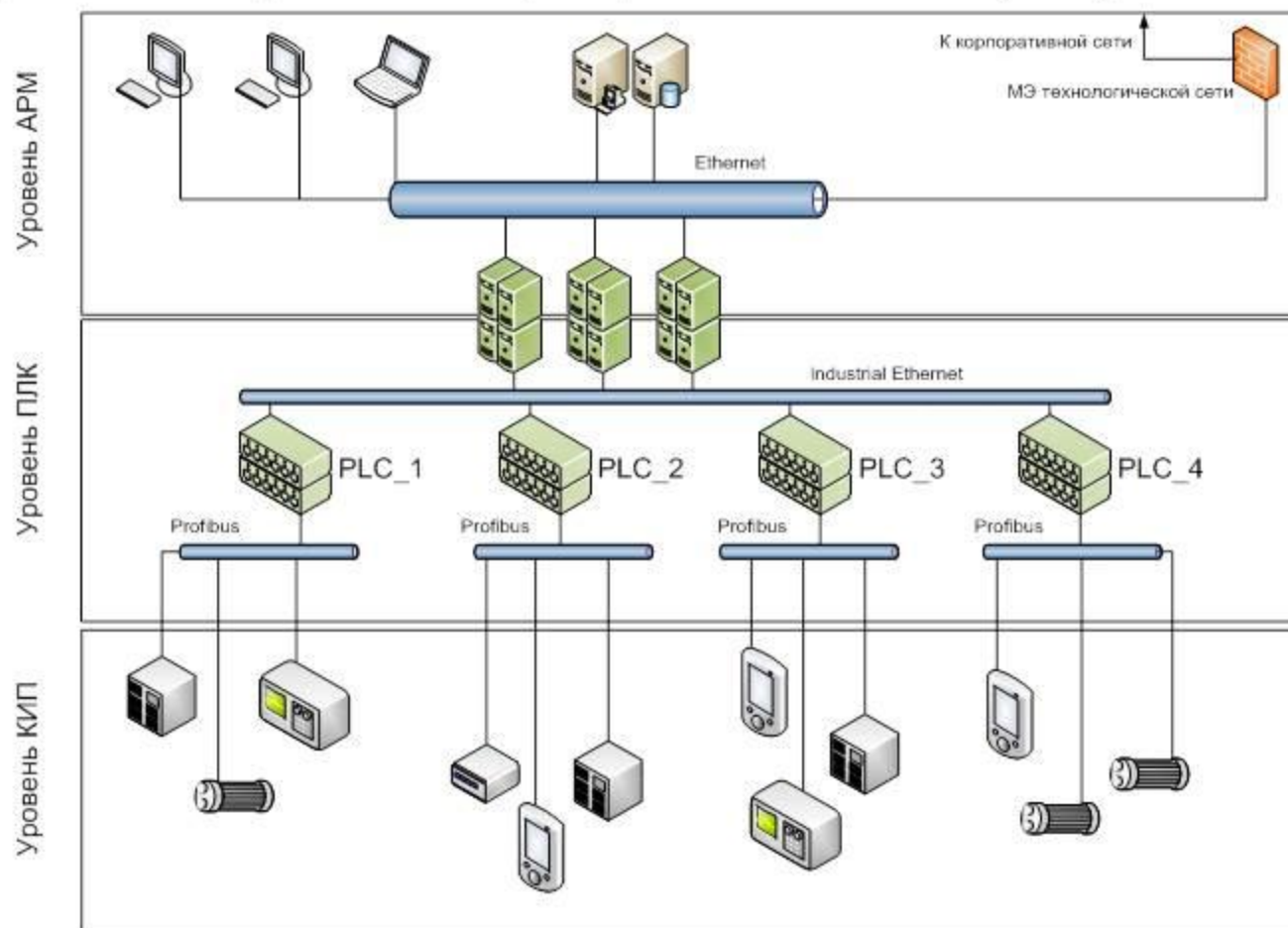
9.6. Система обеспечения ИБ АСУ ТП

9.7. Аттестация АСУ ТП



АСУ ТП представляет собой программно-аппаратный комплекс, состоящий из:

- автоматизированных рабочих мест (станция оператора, станция инженера, станция инженера КИП) – уровень АРМ;
- программируемого логического контроллера (ПЛК);
- контрольно-измерительных приборов и автоматики (КИП).



Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 10

Информационная безопасность и системы физической защиты критически важных объектов (ИБ и СФЗ КВО)



Толстой Александр Иванович

К.Т.Н., доцент

**Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ**



Москва, 2017

Содержание



Тема 10. ИБ и СФЗ КВО:

10.1. Введение

10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте

10.3. Обеспечение безопасности информации в самой СФЗ.

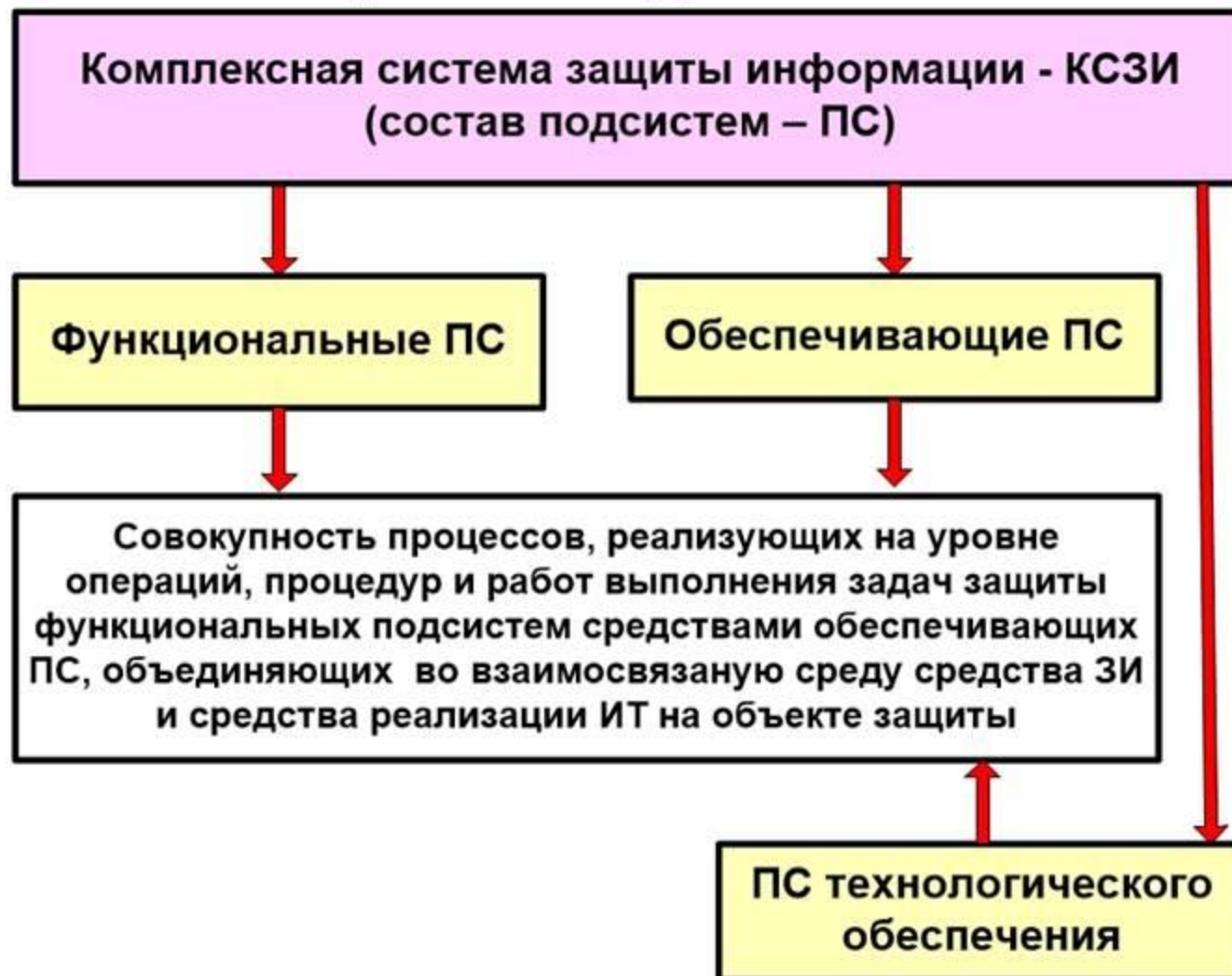
10.4. Обеспечение ИБ СФЗ ядерных объектов

10.5. Обеспечение ИБ систем учета и контроля ядерных материалов

10.6. Обеспечение ИБ при использовании систем связи на ядерных объектах

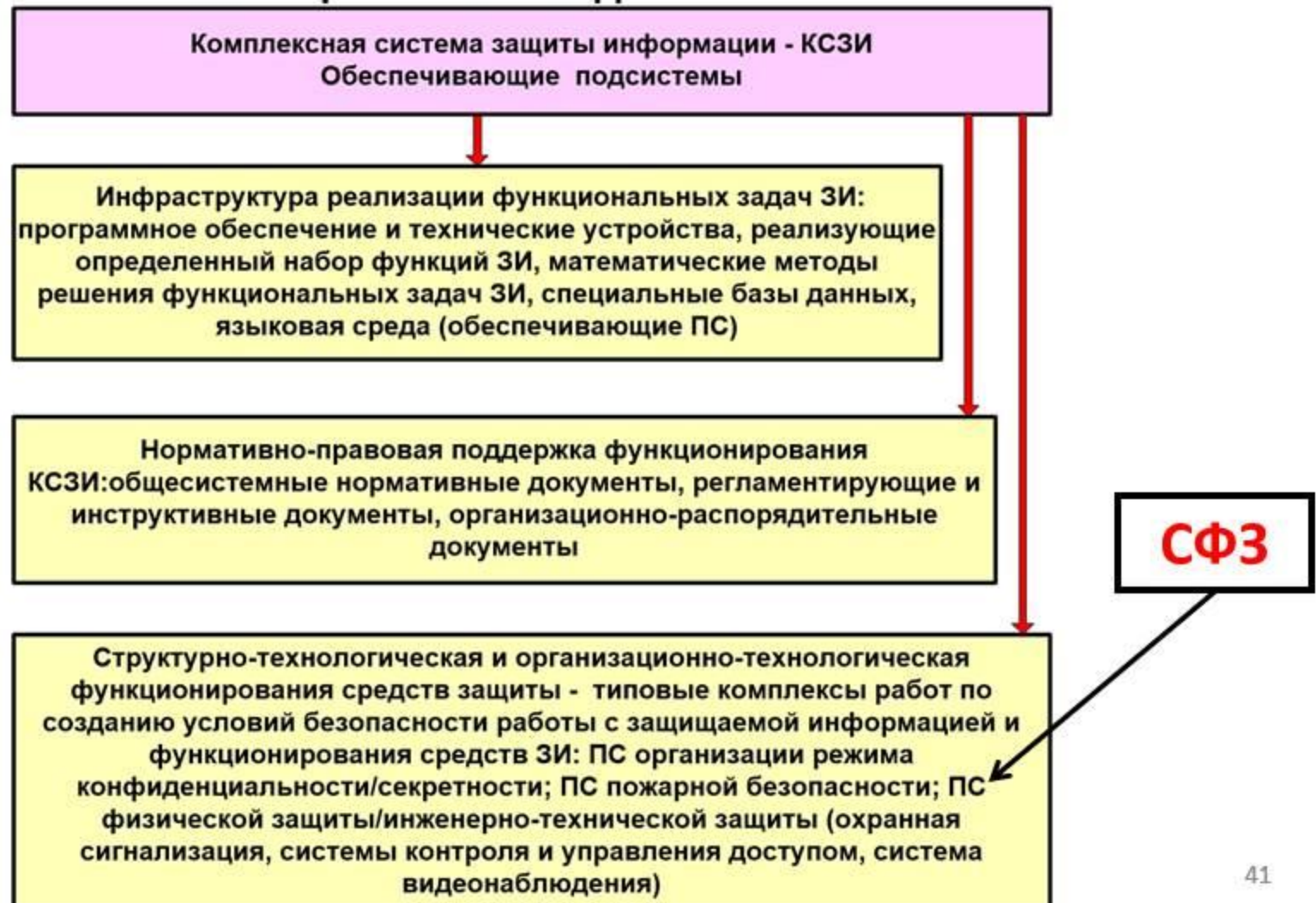
СФЗ как поддерживающая система обеспечения безопасности информации на объекте

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



СФЗ как поддерживающая система обеспечения безопасности информации на объекте

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



Система физической защиты (ФЗ):

Комплекс: инженерно-технических средств и организационных мероприятий, направленных на обеспечение безопасности на объекте.

Совокупность: 1) организационных мероприятий ,
2) инженерно-технических средств, 3) действий подразделений охраны с целью обеспечения безопасности на объекте.

Б (защищаемого объекта) - состояние защищенности объекта от угроз причинения ущерба (вреда).....

(ГОСТ Р 53704-2009 «Системы безопасности комплексные и интегрированные. Общие технические требования»).

Система физической защиты и обеспечение ИБ:

- 1. СФЗ как поддерживающая система обеспечения безопасности информации на объекте**
- 2. Обеспечение безопасности информации в самой СФЗ**

10.2. СФЗ как поддерживающая система обеспечения безопасности информации на объекте:

Дополнительная информация (самостоятельное изучение):

**Физическая защита ядерных объектов: Учебное пособие для вузов/
П.В.Бондарев, А.В.Измайлов, А.И.Толстой; Под ред. Н.С.Погожина.- М.:
МИФИ, 2008.- 584 с.**

Стр. 8 - 32

Глава 1. Методологические основы построения СФЗ объектов

Стр. 298-335

Глава 8. Особенности СФЗ ядерных объектов

10.3. Обеспечение безопасности информации в самой СФЗ

Дополнительная информация (самостоятельное изучение):

**Физическая защита ядерных объектов: Учебное пособие для вузов/
П.В.Бондарев, А.В.Измайлов, А.И.Толстой; Под ред. Н.С.Погожина.- М.:
МИФИ, 2008.- 584 с.**

Глава 8. Особенности СФЗ ядерных объектов

Стр. 298-335

Глава 12. Информационная безопасность СФЗ ядерных объектов

Стр. 389-489

10.4. Обеспечение информационной безопасности СФЗ ядерных объектов

Дополнительная информация (самостоятельное изучение):

**Физическая защита ядерных объектов: Учебное пособие для вузов/
П.В.Бондарев, А.В.Измайлов, А.И.Толстой; Под ред. Н.С.Погожина.- М.:
МИФИ, 2008.- 584 с.**

Глава 8. Особенности СФЗ ядерных объектов

Стр. 298-335

Глава 12. Информационная безопасность СФЗ ядерных объектов

Стр. 389-489

10.6. Обеспечение информационной безопасности при использовании систем связи на ядерных объектах систем учета и контроля ядерных материалов

Дополнительная информация (самостоятельное изучение):

**Физическая защита ядерных объектов: Учебное пособие для вузов/
П.В.Бондарев, А.В.Измайлов, А.И.Толстой; Под ред. Н.С.Погожина.- М.:
МИФИ, 2008.- 584 с.**

**Глава 12. Информационная безопасность СФЗ ядерных объектов
Стр. 389-489**

Благодарю за внимание!

Толстой Александр Иванович

Национальный исследовательский ядерный университет

«МИФИ» (НИЯУ МИФИ)

**кафедра «Информационная безопасность банковских
систем»**

**Институт интеллектуальных кибернетических систем
НИЯУ МИФИ**

AITolstoj@mephi.ru