Московский институт новых информационных технологий

ФСБ России

Федеральное государственное казенная образовательная организация

ДОПОЛНИТЕЛЬНОГО профессионального образования

Московский институт новых информационных технологий ФСБ России

Программа повышения квалификации

«Основы использования новых информационных технологий в управленческой деятельности»

«Основы использования новых информационных технологий в управленческой деятельности»

Цель обучения	повышение квалификации руководителей подразделений органов федеральной службы безопасности и сотрудников, состоящих в резерве выдвижения на должности руководителей.
Категория обучаемых	сотрудники ФСБ России, проходящие военную службу и планирующиеся к назначению на воинские должности, связанные с управленческой деятельностью, имеющие высшее профессиональное образование.
Продолжительность обучения	82 учебных часа.

«Основы использования новых информационных технологий в управленческой деятельности»

Раздел I:

Организационно-правовые основы государственной службы

Раздел II:

Основы технологического обеспечения государственной службы и информатизации

Раздел III:

Основы обеспечения информационной безопасности инфокоммуникационных систем государственной службы

№ п/п	Наименование разделов (модулей), тем, виды занятий	Количество учебных часов								Кафедра, ответственная за проведение занятий, практические подразделения
			Аудиторное время					самостоятельная работа	аттестация	
		Всего часов	всего аудиторных часов	лекции	семинары	ПРЗ	другие виды аудиторных занятий			
1.	Входной контроль. Практическое занятие.	2	2				2			Кафедра № 4
Раздел I: Организационно-правовые основы государственной службы										
1.	**Тема 1: Правовые основы информационной безопасности Российской Федерации.** Лекция	2	2	2						Кафедра № 4
1.	Тема 2: Основы организации государственной службы в Российской Федерации. Семинар.	2	2		2					Кафедра № 4
1.	Тема 3: Сущность информатизации и содержание применения информационных технологий в управленческой деятельности. Лекция	2	2	2						Кафедра № 4
1.	Тема 4: Концепция использования информационных технологий в деятельности органов власти. Лекция	2	2	2						Кафедра № 4
1.	Тема 4: Направления развития цифровой экономики России Семинар	2	2		2					Кафедра № 4
1.	ИТОГО по I разделу									

Тема 1.

Правовые основы информационной безопасности Российской Федерации

Раздел 1. Организационно-правовые основы государственной службы

Тема **1.**
Правовые основы информационной безопасности Российской Федерации

ЛЕКЦИЯ № 1.
Система государственных органов обеспечения национальной безопасности

ЛЕКЦИЯ № 2.
Характеристика информационной безопасности и защиты информации

Тема 1.
Правовые основы информационной безопасности Российской Федерации

ЛЕКЦИЯ № 2.

ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Список литературы:

1. Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств - участников Содружества Независимых Государств в сфере информатизации (Москва, 24 декабря 1999 г.)

2. Федеральный закон Российской Федерации от 27.06.2006 № 149—ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон Российской Федерации от 27.06.2006 № 152—ФЗ «О персональных данных»

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Список литературы:

4. Государственный стандарт Российской Федерации ГОСТ 9126-94. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению.

5. Национальный стандарт Российской Федерации ГОСТ Р 50922—2006. Защита информации. Основные термины и определения.

6. Государственный стандарт Российской Федерации ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Список литературы:

7. **Национальный стандарт Российской Федерации ГОСТ Р 51275—2006.** Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

8. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 12207-2010 "Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств"

9. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Список литературы:

12. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 13335—1—2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

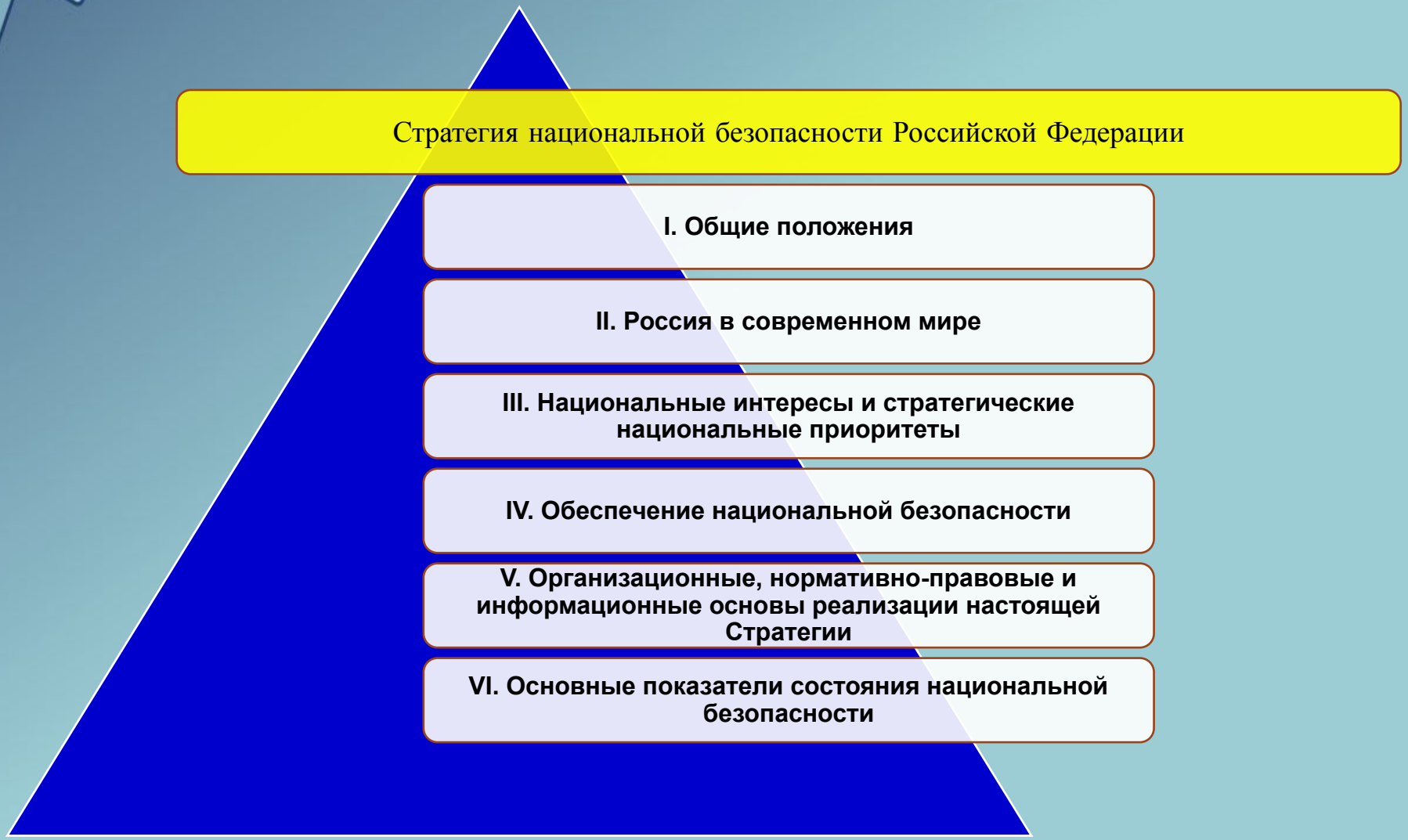
ЛЕКЦИЯ № 2
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Список литературы:

13. Указ Президента Российской Федерации от 31 декабря 2015 г. N 683 "О Стратегии национальной безопасности Российской Федерации"

14. Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ



Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 “Об утверждении Доктрины информационной безопасности Российской Федерации”

Доктрина информационной безопасности Российской Федерации

- I. Общие положения
- II. Национальные интересы в информационной сфере
- III. Основные информационные угрозы и состояние информационной безопасности
- IV. Стратегические цели и основные направления обеспечения информационной безопасности
- V. Организационные основы обеспечения информационной безопасности

Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895)

Преамбула
I. Информационная безопасность РФ (п.п. 1 - 4)
II. Методы обеспечения информационной безопасности РФ (п.п. 5 - 7)
III. Основные положения государственной политики обеспечения информационной безопасности РФ и первоочередные мероприятия по ее реализации (п.п. 8 - 9)
IV. Организационная основа системы обеспечения информационной безопасности РФ (п.п. 10 - 11).

Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646)

I. Общие положения (п.п. 1 - 6)
II. Национальные интересы в информационной сфере (п.п. 7 - 9)
III. Основные информационные угрозы и состояние информационной безопасности (п. п. 10 - 19)
IV. Стратегические цели и основные направления обеспечения информационной безопасности (п.п. 20 - 29)
V. Организационные основы обеспечения информационной безопасности (п.п. 30 - 38)

Доктрина информационной безопасности Российской Федерации

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ **представляет собой СОВОКУПНОСТЬ официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ — состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

ИНФОРМАЦИОННАЯ СФЕРА **(**СРЕДА**)** - сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Соглашение о свободном доступе и порядке обмена открытой научно-технической информацией государств-участников СНГ (Москва, 11 сентября 1998 г.)

ДОКТРИНА **представляет собой СИСТЕМУ официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.**

ИНФОРМАЦИОННАЯ СФЕРА **— совокупность информации, объектов информатизации, информационных систем, сайтов в ИТКС “Интернет”, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ **— состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;**

Доктрина информационной безопасности Российской Федерации

Интересы личности в информационной сфере **заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.**

Интересы общества в информационной сфере **заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.**

Интересы государства в информационной сфере **заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.**

Национальные интересы Российской Федерации в информационной сфере - **объективно значимые потребности**

- **личности,**
- **общества**
- **государства**

в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы.

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Список литературы:

14. Р 50.1.053—2005 Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации.

15. Р 50.1.056—2005 Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения.

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Цель занятия: рассмотреть и проанализировать структуру и содержание терминов «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» и «ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 1. Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ВОПРОС 2. Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 3. Виды защиты информации

ВОПРОС 4. Защищаемые объекты

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

ВОПРОС 1.

Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Различают термин «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» в узком смысле этого слова и в широком смысле.

Рассмотрим первоначально в узком смысле, что означает термин «Информационная безопасность» и параметры, ее описывающие.

При рассмотрении мы будем руководствоваться действующей нормативной базой Российской Федерации.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — информационная безопасность (information security): защита

— конфиденциальности,

— целостности

— доступности информации;

— кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — информационная безопасность (information security): защита

— конфиденциальности,

— целостности

— доступности информации;

— кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

КОНФИДЕНЦИАЛЬНОСТЬ — свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса

ГОСТ Р ИСО/МЭК 13335-1-2006, ст.2.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

(Федеральный закон «Об информации, информационных технологиях и о защите информации», ст. 2).

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Конфиденциальность информации [ресурсов автоматизированной информационной системы]) — состояние информации [ресурсов автоматизированной информационной системы], при котором доступ к ней [к ним] осуществляют только субъекты, имеющие на него право

(Р 50.1.053-2005, ст. 3.1.7).

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания

(Федеральный закон «О персональных данных», ст. 3) .

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — информационная безопасность (information security): защита

— конфиденциальности,

— целостности

— доступности информации;

— кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ЦЕЛОСТНОСТЬ — состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

ГОСТ Р 50922-2006, пр. А.17.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ — состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

(Р 50.1.056-2005, ст. 3.1.6).

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Целостность (информации [ресурсов автоматизированной информационной системы]) — состояние информации [ресурсов автоматизированной информационной системы], при котором ее [их] изменение осуществляется только преднамеренно субъектами, имеющими на него право

Р 50.1.053-2005, ст. 3.1.8.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — информационная безопасность (information security): защита

— конфиденциальности,

— целостности

— доступности информации;

— кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ДОСТУПНОСТЬ — свойство быть доступным и используемым по запросу со стороны уполномоченного логического объекта.

ГОСТ Р ИСО/МЭК 7498-2-99, ст.3.3.11.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Доступность (информации [ресурсов автоматизированной информационной системы]) — состояние информации [*ресурсов* автоматизированной информационной системы], при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно

(Р 50.1.053-2005, ст. 3.1.9).

***ПРИМЕЧАНИЕ*:**

К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ИНФОРМАЦИОННЫЕ РЕСУРСЫ — отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов)

(ГОСТ Р 51275-2006, ст. 2.1).

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Защищаемые информационные ресурсы (автоматизированной информационной системы) — информационные ресурсы автоматизированной информационной системы, для которых должен быть обеспечен требуемый уровень их защищенности)

(Р 50.1.053-2005, ст.3.1.2.).

***ПРИМЕЧАНИЕ*:**

Информационные ресурсы включают в себя документы и массивы документов, используемые в автоматизированных информационных системах

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Информационные ресурсы сети электросвязи, требующие защиты со стороны оператора связи (ГОСТ Р 52448-2005, ст.5.1):

- **сведения об абонентах, базы данных;**
- **информация управления;**
- **данные, содержащие информацию пользователей (обеспечение доступности и целостности);**
- **программное обеспечение систем управления сетями электросвязи;**
- **сведения о прохождении, параметрах, загрузке (использовании) линий связи магистральных сетей;**
- **обобщенные сведения о местах дислокации узлов связи и установленном сетевом оборудовании;**
- **сведения, раскрывающие структуру используемых механизмов обеспечения БЕЗОПАСНОСТИ сети электросвязи.**

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — информационная безопасность (information security): защита

— конфиденциальности,
— целостности
— доступности информации;
— кроме того, сюда могут быть отнесены и другие свойства, например
— аутентичность,
— подотчетность,
— неотказуемость
— и надежность.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — все аспекты, связанные с определением, достижением и поддержанием

- **конфиденциальности,**
- **целостности,**
- **доступности,**
- **неотказуемости,**
- **подотчетности,**
- **аутентичности и**
- **достоверности информации или средств ее обработки**

(ГОСТ Р ИСО/МЭК 13335-1-2006, ст. 2.14).

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Из определения видно, что ряд параметров, описывающих термин, уже нами рассмотрены, так как входят в определение ИБ в узком смысле этого слова.

Далее рассмотрим параметры, которые дополнительно дают уточняющую характеристику данного термина:

- НЕОТКАЗУЕМОСТЬ,
- ПОДОТЧЕТНОСТЬ,
- АУТЕНТИЧНОСТЬ.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Из определения видно, что ряд параметров, описывающих термин, уже нами рассмотрены, так как входят в определение ИБ в узком смысле этого слова.

Далее рассмотрим параметры, которые дополнительно дают уточняющую характеристику данного термина:

- НЕОТКАЗУЕМОСТЬ,
- ПОДОТЧЕТНОСТЬ,
- АУТЕНТИЧНОСТЬ.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

НЕОТКАЗУЕМОСТЬ - способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты

(ГОСТ Р ИСО/МЭК 13335-1-2006, ст. 2.16).

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Далее продолжим рассмотрение параметров, которые дополнительно дают уточняющую характеристику данного термина:

НЕОТКАЗУЕМОСТЬ,

ПОДОТЧЕТНОСТЬ,

АУТЕНТИЧНОСТЬ.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ПОДОТЧЕТНОСТЬ - свойство, обеспечивающее однозначное прослеживание действий любого логического объекта

(ГОСТ Р ИСО/МЭК 13335-1-2006, ст. 2.1).

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Подотчетность (ресурсов автоматизированной информационной системы) - **состояние ресурсов автоматизированной информационной системы, при котором обеспечиваются их идентификация и регистрация**

(Р 50.1.053-2005, ст. 3.1.10).

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Далее продолжим рассмотрение параметров, которые дополнительно дают уточняющую характеристику данного термина:

НЕОТКАЗУЕМОСТЬ,
ПОДОТЧЕТНОСТЬ,
АУТЕНТИЧНОСТЬ.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

АУТЕНТИЧНОСТЬ - свойство, гарантирующее, что субъект или ресурс идентичны заявленным
(ГОСТ Р ИСО/МЭК 13335-1-2006, ст. 2.3).

***ПРИМЕЧАНИЕ*:**

Аутентичность применяется к таким субъектам, как пользователи, к процессам, системам и информации.

Национальный стандарт Российской Федерации
ГОСТ Р ИСО/МЭК 27002-2012
"Информационная технология.
Методы и средства обеспечения безопасности.
Свод норм и правил менеджмента информационной безопасности"

2.5 **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ** (information security) — **защита**

- **конфиденциальности,**
- **целостности**
- **доступности информации;**

кроме того,
сюда могут быть отнесены и другие свойства,
НАПРИМЕР:

- **аутентичность,**
- **подотчетность,**
- **неотказуемость и**
- **НАДЕЖНОСТЬ.**

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

НАДЕЖНОСТЬ автоматизированной системы — комплексное свойство АС сохранять во времени в установленных пределах значения всех ПАРАМЕТРОВ, характеризующих способность АС выполнять свои функции в заданных режимах и условиях эксплуатации.

ПРИМЕЧАНИЕ.

Надежность АС включает свойства безотказности и ремонтопригодности АС, а в некоторых случаях и долговечности технических средств АС.

ГОСТ 34.003-90, ст. 3.11.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Техническое обслуживание, направленное на обеспечение НАДЕЖНОСТИ **(RCM), является**

методом определения Политики проведения технического обслуживания, **направленной на предупреждение отказов и способов ее внедрения для достижения:**

— необходимого уровня *БЕЗОПАСНОСТИ*,

— эксплуатационной готовности

— и экономичности функционирования для всех типов оборудования.

Национальный стандарт РФ ГОСТ Р ИСО/МЭК 31010-2011"Менеджмент риска. Методы оценки риска"

Благодаря глубокому исследованию риска оценка риска помогает ЛИЦАМ, ПРИНИМАЮЩИМ РЕШЕНИЯ, и ответственным сторонам:

— влиять на достижение поставленных целей,

— выбирать адекватные и эффективные средства управления риском.

Оценка риска является основой для принятия решений по обработке риска.

Выходные данные процесса оценки риска являются входными данными процессов принятия решений в организации.

Оценка риска является процессом, объединяющим идентификацию, анализ риска и сравнительную оценку риска (см. рисунок 1).

Способ реализации этого процесса зависит не только от области применения процесса менеджмента риска, но также и от методов оценки риска.

Национальный стандарт РФ ГОСТ Р ИСО/МЭК 31010-2011"Менеджмент риска. Методы оценки риска"

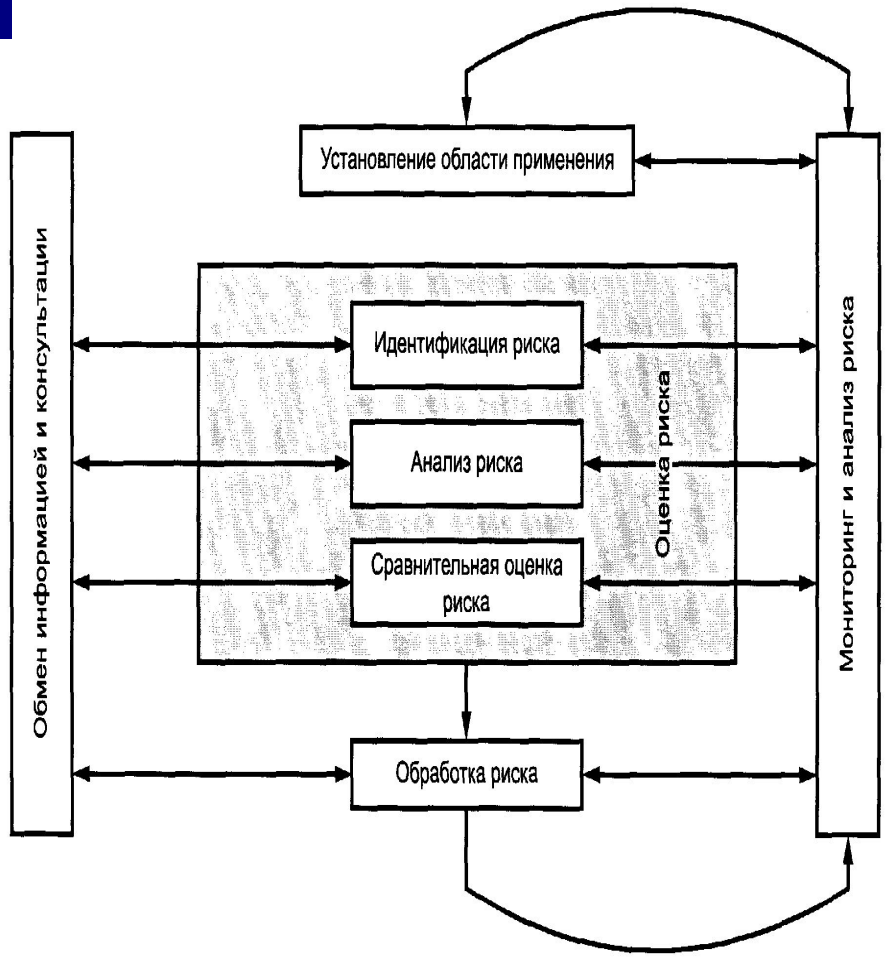


Рис. 1. Идентификация риска

Независимо от фактически используемых методов при идентификации риска важно учитывать человеческие и организационные факторы.

Отклонения, вызванные воздействием человеческих и организационных факторов, а также

ОПАСНЫЕ СОБЫТИЯ, СВЯЗАННЫЕ С ИНФОРМАЦИОННЫМИ ТЕХНОЛОГИЯМИ,

должны быть учтены в процессе идентификации риска.

Национальный стандарт РФ ГОСТ Р ИСО/МЭК 31010-2011" Менеджмент риска. Методы оценки риска"

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

СОБЫТИЕ — возникновение или наличие определенной совокупности обстоятельств.

***ПРИМЕЧАНИЯ*:**

1 Характер, вероятность и последствия события могут быть не полностью известны.

2 Событие может возникать один или несколько раз.

3 Вероятность, связанная с событием, может быть оценена.

4 Событие может состоять из невозникновения одного или нескольких обстоятельств.

5 Непредсказуемое событие иногда называют «ИНЦИДЕНТОМ».

6 Событие, при котором не происходит никаких потерь, иногда называют предпосылкой к происшествию [инциденту], опасным состоянием, опасным стечением обстоятельств и т.д.

ГОСТ Р 53114-2008, ст.3.2.8

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

СОБЫТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

— какое-либо событие информационной безопасности, идентифицируемое появлением определенного состояния системы, сервиса или сети, указывающее:

— на возможное нарушение политики информационной безопасности

— или отказ защитных мер,

— или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

ГОСТ Р ИСО/МЭК 27002-2012

ИНЦИДЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(information security incident) — любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

***ПРИМЕЧАНИЕ*:**

Инцидентами информационной безопасности являются:

1. **утрата услуг, оборудования или устройств;**
2. **системные сбои или перегрузки;**
3. **ошибки пользователей;**
4. **несоблюдение политики или рекомендаций по ИБ;**
5. **нарушение физических мер защиты,**
6. **неконтролируемые изменения систем;**
7. **сбои программного обеспечения и отказы технических средств;**
8. **нарушение правил доступа.**

ГОСТ Р ИСО/МЭК 27001-2012
ГОСТ Р 53114-2008

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

И так, резюмируя анализ определения и входящих в него характеристик, можно продолжить для полноты картины ДЕЙСТВУЮЩИМ ТЕРМИНОМ, который характеризует информационную безопасность на территории Российской Федерации:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТА ИНФОРМАТИЗАЦИИ —

состояние защищенности объекта информатизации,

при котором обеспечивается безопасность информации и автоматизированных средств ее обработки

Р 50.1.056-2005, ст. 3.1.1.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ОБЪЕКТ ИНФОРМАТИЗАЦИИ — совокупность

- **информационных ресурсов,**
- **средств и систем обработки информации, используемых в соответствии с заданной информационной технологией,**
- **средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены,**
- **или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.**

ГОСТ Р 51275-2006, ст. 2.1.

ВОПРОС 1.
Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Информационная безопасность Российской Федерации — состояние *ЗАЩИЩЕННОСТИ*

- **личности,**
- **общества и**
- **государства**

от внутренних и внешних информационных УГРОЗ,
при котором обеспечиваются:
— реализация конституционных прав и свобод человека и гражданина,
— достойные качество и уровень жизни граждан,
— суверенитет,
— территориальная целостность
— и устойчивое социально-экономическое развитие Российской Федерации,

- **оборона**
- **и БЕЗОПАСНОСТЬ государства.**

Доктрина информационной безопасности Российской Федерации, раздел 1.

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Цель занятия: рассмотреть и проанализировать структуру и содержание терминов «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» и «ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 1. Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ВОПРОС 2. Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 3. Виды защиты информации

ВОПРОС 4. Защищаемые объекты

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

ВОПРОС 2.

Характеристика термина

«ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА (защищенность) (security)

— предохранение информации и данных с тем,

- **чтобы неуполномоченные лица или системы не могли их читать или изменять,**
- **а уполномоченным лицам или системам не было отказано в доступе к ним.**

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств», ст. 4.39

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — все средства и функции, обеспечивающие

— доступность,

— конфиденциальность

— или целостность информации или связи,

исключая средства и функции, предохраняющие от неисправностей.

Она включает в себя криптографию, криптоанализ, защиту от собственного излучения и защиту компьютера.

Указ Президента Российской Федерации от 17 декабря 2011 г. N 1661 "Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль"

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — все средства и функции, обеспечивающие

— **доступность**,

— **КОНФИДЕНЦИАЛЬНОСТЬ**

— или **ЦЕЛОСТНОСТЬ** информации или связи,

исключая средства и функции, предохраняющие от неисправностей.

Она включает в себя криптографию, криптоанализ, защиту от собственного излучения и защиту компьютера.

Указ Президента Российской Федерации от 17 декабря 2011 г. N 1661 "Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль"

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — все средства и функции, обеспечивающие
- **доступность**,
- **конфиденциальность**
- или **целостность**

информации или связи, исключая средства и функции, предохраняющие от неисправностей.

Она включает в себя криптографию, криптоанализ, защиту от собственного излучения и защиту компьютера.

Указ Президента Российской Федерации от 17 декабря 2011 г. N 1661

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — все аспекты, связанные с определением, достижением и поддержанием
- **конфиденциальности,**
- **целостности,**
- **доступности,**
- **неотказуемости,**
- **подотчетности,**
- **аутентичности и**
- **достоверности информации или средств ее обработки**

ГОСТ Р ИСО/МЭК 13335-1-2006

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — все средства и функции, обеспечивающие
— доступность,
— конфиденциальность
— или **ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ** или связи,
исключая средства и функции, предохраняющие от неисправностей.

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ — состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Р 50.1.056—2005 Рекомендации по стандартизации.
Техническая защита информации. Основные термины и определения.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — все средства и функции, обеспечивающие доступность, конфиденциальность или целостность информации или связи, исключая средства и функции, предохраняющие от неисправностей.

Она включает в себя криптографию, криптоанализ, защиту от собственного излучения и защиту компьютера.

Указ Президента Российской Федерации от 17 декабря 2011 г. N 1661 "Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль"

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

Она включает в себя **КРИПТОГРАФИЮ**, криптоанализ, защиту от собственного излучения и защиту компьютера.

Указ Президента Российской Федерации от 17 декабря 2011 г. N 1661

ТЕХНИЧЕСКОЕ ПРИМЕЧАНИЕ:

КРИПТОГРАФИЯ — дисциплина, включающая принципы, средства и методы преобразования информации в целях сокрытия ее содержания, предотвращения ее неподдающегося обнаружению видоизменения или несанкционированного использования.

Криптография ограничена преобразованием информации с использованием одного или более *СЕКРЕТНЫХ ПАРАМЕТРОВ* (например, криптографических переменных) или соответствующим управлением ключом.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

Она включает в себя КРИПТОГРАФИЮ, криптоанализ, защиту от собственного излучения и защиту компьютера.

Указ Президента Российской Федерации от 17 декабря 2011 г. N 1661 "Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль"

ТЕХНИЧЕСКОЕ ПРИМЕЧАНИЕ:

СЕКРЕТНЫЙ ПАРАМЕТР - константа или ключ, скрываемый от знания других или известный только определенному кругу лиц.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

Указ Президента Российской Федерации от 17 декабря 2011 г. N 1661 "Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль«

ТЕХНИЧЕСКОЕ ПРИМЕЧАНИЕ:

КВАНТОВАЯ КРИПТОГРАФИЯ — совокупность технических приемов по созданию совместно используемого ключа для защиты информации путем измерения квантово-механических свойств физической системы (включая те физические свойства, которые ясно определены квантовой оптикой, квантовой теорией поля или квантовой электродинамикой).

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

Она включает в себя КРИПТОГРАФИЮ, криптоанализ, защиту от собственного излучения и защиту компьютера.

КРИПТОГРАФИЯ — дисциплина, охватывающая принципы, средства и методы преобразования данных для сокрытия их информационного содержимого, предотвращения их необнаруживаемой модификации и/или их несанкционированного использования

Государственный стандарт РФ ГОСТ Р ИСО 7498-2-99
"Информационная технология. Взаимосвязь открытых систем.
Базовая эталонная модель.
Часть 2. Архитектура защиты информации"

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

Она включает в себя **КРИПТОГРАФИЮ**, криптоанализ, защиту от собственного излучения и защиту компьютера.

КРИПТОГРАФИЯ устанавливает методы, используемые при шифровании и дешифровании.

Любое вторжение в криптографические принципы, средства или методы, представляет собой *КРИПТОАНАЛИЗ*.

Государственный стандарт РФ ГОСТ Р ИСО 7498-2-99
"Информационная технология. Взаимосвязь открытых систем.
Базовая эталонная модель.
Часть 2. Архитектура защиты информации"

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — все средства и функции, обеспечивающие доступность, конфиденциальность или целостность информации или связи, исключая средства и функции, предохраняющие от неисправностей.

Она включает в себя КРИПТОГРАФИЮ, КРИПТОАНАЛИЗ, защиту от собственного излучения и защиту компьютера.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

Указ Президента Российской Федерации от 17 декабря 2011 г. N 1661 "Об утверждении Списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль"

ТЕХНИЧЕСКОЕ ПРИМЕЧАНИЕ:

КРИПТОАНАЛИЗ — анализ криптографической системы и/или ее входов и выходов с целью получения конфиденциальных переменных и/или чувствительных данных, включая открытый текст.

Государственный стандарт Российской Федерации ГОСТ Р ИСО 7498-2-99 "Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации"

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ —
все средства и функции, обеспечивающие доступность, конфиденциальность или целостность информации или связи, исключая средства и функции, предохраняющие от неисправностей.

Она включает в себя криптографию, криптоанализ, ЗАЩИТУ ОТ СОБСТВЕННОГО ИЗЛУЧЕНИЯ и защиту компьютера.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ОТ СОБСТВЕННОГО ИЗЛУЧЕНИЯ

Оборудование должно обеспечивать защиту от генерируемого им и представляющего опасность электромагнитного излучения, а также от звукового и ультразвукового давления.

Соответствие требованию проверяют, если оборудование имеет указанные источники опасности.

Государственный стандарт Российской Федерации
ГОСТ Р 51350-99 (МЭК 61010-1-90)
"Безопасность электрических контрольно-измерительных приборов и лабораторного оборудования.
Часть 1. Общие требования"

ВОПРОС 2.

Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — все средства и функции, обеспечивающие доступность, конфиденциальность или целостность информации или связи, исключая средства и функции, предохраняющие от неисправностей.

Она включает в себя криптографию, криптоанализ, защиту от собственного излучения и ЗАЩИТУ КОМПЬЮТЕРА.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — ЗАЩИТА КОМПЬЮТЕРА.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА; ЗИ от НСД:

— Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

***ПРИМЕЧАНИЕ* - Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.**

ГОСТ Р 50922—2006 Защита информации. Основные термины и определения.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — ЗАЩИТА КОМПЬЮТЕРА.

ЗАЩИТА ИНФОРМАЦИИ ОТ ПРЕДНАМЕРЕННОГО ВОЗДЕЙСТВИЯ; ЗИ от ПДВ:

Защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

ГОСТ Р 50922—2006 Защита информации. Основные термины и определения.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — ЗАЩИТА КОМПЬЮТЕРА.

ЗАЩИТА ПРОГРАММНЫХ СРЕДСТВ **- организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий.**

Государственный стандарт Российской Федерации
ГОСТ Р 51188-98.
Защита информации.
Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — ЗАЩИТА КОМПЬЮТЕРА.

ЗАЩИТА ИНФОРМАЦИИ ОТ [ИНОСТРАННОЙ] РАЗВЕДКИ: ***Защита информации, направленная на предотвращение получения защищаемой информации [иностранной] разведкой.***

ГОСТ Р 50922—2006
Защита информации.
Основные термины и определения.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — ЗАЩИТА КОМПЬЮТЕРА.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ВОЗДЕЙСТВИЯ; ЗИ от НСВ:

Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

ГОСТ Р 50922—2006 Защита информации. Основные термины и определения.

ВОПРОС 2.
Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ЗАЩИТА ИНФОРМАЦИИ — ЗАЩИТА КОМПЬЮТЕРА.

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕПРЕДНАМЕРЕННОГО ВОЗДЕЙСТВИЯ —

Защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

ГОСТ Р 50922—2006 Защита информации. Основные термины и определения.

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Цель занятия: рассмотреть и проанализировать структуру и содержание терминов «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» и «ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 1. Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ВОПРОС 2. Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 3. Виды защиты информации

ВОПРОС 4. Защищаемые объекты

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

ВОПРОС 3.

Виды защиты информации

ВОПРОС 3.
Виды защиты информации

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

— обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

— соблюдение конфиденциальности информации ограниченного доступа,

— реализацию права на доступ к информации.

Федеральный закон «Об информации, информационных технологиях и о защите информации», ст. 16.

ВОПРОС 3.
Виды защиты информации

ЗАЩИТА ИНФОРМАЦИИ - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

(ГОСТ Р 50922—2006, ст.2.1.1).

При этом стандартом ГОСТ Р 50922-2006 установлены термины, относящиеся к ВИДАМ ЗАЩИТЫ ИНФОРМАЦИИ:

- **2.2.1 правовая защита информации:**
- **2.2.2 техническая защита информации;**
- **2.2.3 криптографическая защита информации:**
- **2.2.4 физическая защита информации**:

ВОПРОС 3.
Виды защиты информации

ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ:

2.2.1 правовая защита информации:

Защита информации правовыми методами, включающая в себя
— разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации,
— применение этих документов (актов),
— а также надзор и контроль за их исполнением.

ВОПРОС 3.
Виды защиты информации

ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ:

2.2.1 правовая защита информации:

2.2.2 техническая защита информации;

2.2.3 криптографическая защита информации:

2.2.4 физическая защита информации:

ВОПРОС 3.
Виды защиты информации

ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ:

2.2.2 техническая защита информации;

Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением:

— технических,

— программных

—и программно-технических средств.

ВОПРОС 3.
Виды защиты информации

ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ:

2.2.1 правовая защита информации:

2.2.2 техническая защита информации;

2.2.3 криптографическая защита информации:

2.2.4 физическая защита информации:

ВОПРОС 3.
Виды защиты информации

ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ:

2.2.3 криптографическая защита информации:

Защита информации с помощью ее криптографического преобразования.

ВОПРОС 3.
Виды защиты информации

ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ:

2.2.1 правовая защита информации:

2.2.2 техническая защита информации;

2.2.3 криптографическая защита информации:

2.2.4 физическая защита информации:

ВОПРОС 3.
Виды защиты информации

ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ:

2.2.4 физическая защита информации:

Защита информации путем применения:

— организационных мероприятий

— и совокупности средств,

создающих препятствия для

- **проникновения**
- **или доступа неуполномоченных физических лиц к объекту защиты.**

ВОПРОС 3.
Виды защиты информации

ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ:

2.2.4 физическая защита информации:

ПРИМЕЧАНИЯ

1. **Организационные мероприятия по обеспечению физической защиты информации предусматривают установление:**

— режимных,
— временных,
— территориальных,
— пространственных ограничений
на условия использования и распорядок работы объекта защиты.

2. К объектам защиты информации могут быть отнесены:

- **охраняемая территория,**
- **здание (сооружение),**
- **выделенное помещение,**
- **информация и (или) информационные ресурсы объекта информатизации.**

ВОПРОС 3.
Виды защиты информации

ВИДЫ ЗАЩИТЫ ИНФОРМАЦИИ:

2.2.1 правовая защита информации:

2.2.2 техническая защита информации;

2.2.3 криптографическая защита информации:

2.2.4 физическая защита информации:

ЛЕКЦИЯ № 2.
ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Цель занятия: рассмотреть и проанализировать структуру и содержание терминов «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» и «ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 1. Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ВОПРОС 2. Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 3. Виды защиты информации

ВОПРОС 4. Защищаемые объекты

ВОПРОС 4.

Защищаемые объекты

ВОПРОС 4.

Защищаемые объекты

Защищаемая автоматизированная информационная система — автоматизированная информационная система, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности.

Р 50.1.053—2005 Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации

ВОПРОС 4.

Защищаемые объекты

ЗАЩИЩАЕМАЯ ИНФОРМАЦИОННАЯ СИСТЕМА – **информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.**

Р 50.1.056—2005 Рекомендации по стандартизации. Техническая защита информации.

Основные термины и определения.

ВОПРОС 4.

Защищаемые объекты

ЗАЩИЩАЕМАЯ ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ –

информационная технология, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности.

Р 50.1.053—2005 Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации

ВОПРОС 4.

Защищаемые объекты

ЗАЩИЩЕННОСТЬ —
атрибуты программного обеспечения, относящиеся к его способности предотвращать несанкционированный доступ, случайный или преднамеренный, к программам и данным.

Государственный стандарт Российской Федерации
ГОСТ Р 9126-94.
Информационная технология.
Оценка программной продукции.
Характеристики качества и руководства по их применению.

ВОПРОС 4.

Защищаемые объекты

ЗАЩИЩАЕМАЯ ИНФОРМАЦИЯ –
информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации

ПРИМЕЧАНИЕ:
Собственником информации может быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

ГОСТ Р 51275—2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ВОПРОС 4.

Защищаемые объекты

ЗАЩИЩАЕМЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ (АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ) — **информационные ресурсы автоматизированной информационной системы, для которых должен быть обеспечен требуемый уровень их защищенности)**

***ПРИМЕЧАНИЕ*:**

Информационные ресурсы включают в себя документы и массивы документов, используемые в автоматизированных информационных системах.

Р 50.1.053—2005 Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации

ВОПРОС 4.

Защищаемые объекты

ЗАЩИЩАЕМЫЙ ОБЪЕКТ ИНФОРМАТИЗАЦИИ

— объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

Р 50.1.056—2005 Рекомендации по стандартизации. Техническая защита информации.

Основные термины и определения.

ВОПРОС 4.

Защищаемые объекты

ЗАЩИЩАЕМЫЕ ПРОГРАММНЫЕ СРЕДСТВА – программные средства, используемые в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности.

Р 50.1.056—2005 Рекомендации по стандартизации. Техническая защита информации.

Основные термины и определения.

ВОПРОС 4.

Защищаемые объекты

ЗАЩИЩАЕМЫЕ РЕСУРСЫ (ИНФОРМАЦИОННОЙ СИСТЕМЫ) — ресурсы, использующиеся в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности.

Р 50.1.056—2005 Рекомендации по стандартизации. Техническая защита информации.

Основные термины и определения.

ВОПРОС 4.

Защищаемые объекты

ЗАЩИЩАЕМАЯ СЕТЬ СВЯЗИ —
сеть связи, используемая при обмене защищаемой информацией с требуемым уровнем ее защищенности.

Р 50.1.056—2005 Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения.

ВОПРОС 4.

Защищаемые объекты

ЗНАЧИМЫЙ ОБЪЕКТ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

Федеральный закон от 26 июля 2017 г. N 187-ФЗ"О безопасности критической информационной инфраструктуры Российской Федерации"

ВОПРОС 4.

Защищаемые объекты

"Защищенная от подделок полиграфическая продукция" — полиграфическая продукция, содержащая не менее двух защитных элементов, изготовленная с применением полиграфических, голографических, информационных, микропроцессорных и иных способов защиты полиграфической продукции, предотвращающих подделку этой продукции;

Постановление Правительства Российской Федерации от 24 сентября 2012 г. N 965 "О лицензировании деятельности по производству и реализации защищенной от подделок полиграфической продукции"

ЛЕКЦИЯ № 2.

ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Цель занятия: рассмотреть и проанализировать структуру и содержание терминов «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» и «ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 1. Характеристика термина «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

ВОПРОС 2. Характеристика термина «ЗАЩИТА ИНФОРМАЦИИ»

ВОПРОС 3. Виды защиты информации

ВОПРОС 4. Защищаемые объекты

ЛЕКЦИЯ № 2.

ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

СПАСИБО ЗА ВНИМАНИЕ