Основы информационной безопасности критически важных объектов

Учебная дисциплина ОИБ КВО

Тема 2

Базовая терминология

Толстой Александр Иванович
к.т.н., доцент
Кафедра «Информационная безопасность банковских систем»
Институт интеллектуальных кибернетических систем
НИЯУ МИФИ

Москва, 2017

Р. Декарт:
"Дайте понятиям точное толкование, и вы освободите мир от половины заблуждений»

В.А.Герасименко (высказывание)
«Дискуссии на терминологические темы – самые непродуктивные дискуссии»

Термин:

Слово или словосочетание специальной сферы употребления, являющееся наименованием понятия

Рекомендации по основным принципам и методам стандартизации терминологии РМГ 19-96 (приняты Межгосударственным Советом по стандартизации, метрологии и сертификации (протокол от 04.10.1996 № 10), утверждены Госстандартом России)

Термин называет специальное понятие и в совокупности с другими терминами данной системы является компонентом научной теории определенной области знания.

Требования, предъявляемые к терминам:

- **однозначность соответствия между термином и понятием;**
- **краткость;**
- **системность;**
- **деривационная способность;**
- **лингвистическая правильность**

Определение:

Логический прием, позволяющий установить четкие границы понятия и его место в системе понятий.

Результатом определения является перечень наиболее существенных отличительных признаков понятия, формулируемый в виде предложения (т.е. определение – это лаконичное объяснение и раскрытие значения термина)

Требования, предъявляемые к определениям:

- включение в определение только существенных признаков;
- недопустимость тавтологии;
- системность;
- однозначность понимания; оптимальная краткость;
- непротиворечивость терминам в разных источниках;
- лингвистическая правильность

Источники терминологии:

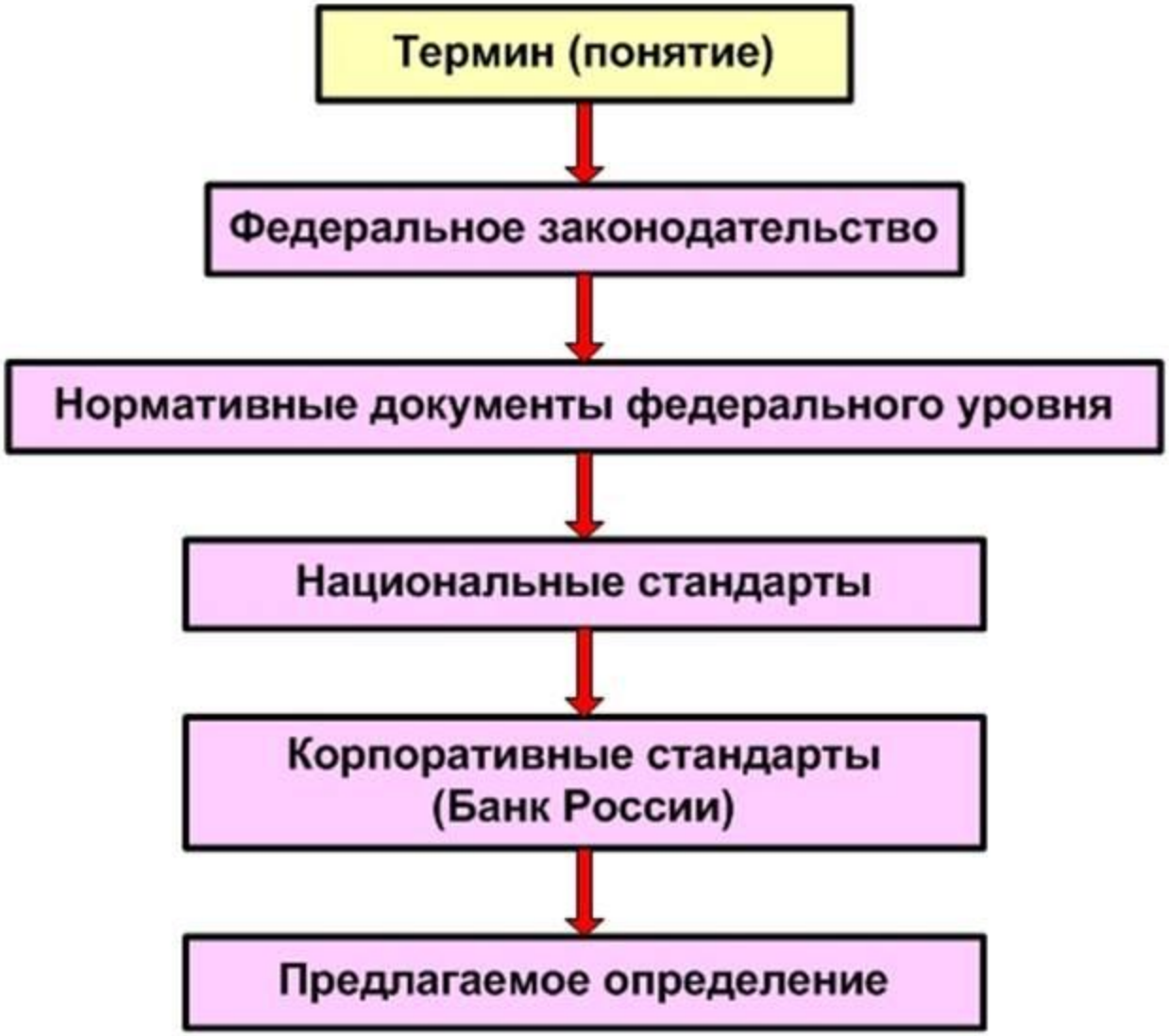
1. **Первичные (неофициальные - незафиксированная терминология): сложившаяся на данный момент.**

2. **Первичная (официальная - зафиксированная терминология):**

- **законодательство;**
- **нормативные документы государственного уровня;**
- **лучшие практики (стандарты, рекомендации в области стандартизации);**
- **лучшие практики (отраслевые нормативные документы).**

3. Вторичные (различные публикации): терминологические словари, справочники, сайты (например, Wikipedia).

Порядок рассмотрения терминов



Р. Декарт:
"Дайте понятиям точное толкование, и вы освободите мир от половины заблуждений»

Основы информационной безопасности критически важных объектов

Информационная безопасность

Р. Декарт:
"Дайте понятиям точное толкование, и вы освободите мир от половины заблуждений»

Основы информационной безопасности критически важных объектов

- Информационная безопасность
- Критически важные объекты

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

↓

Эволюция понятия (с 1970г.)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Эволюция понятия (с 1970г.)

«безопасность данных» (англ. data security),
«компьютерная безопасность» (computer security),
«безопасность информации» или «информационная безопасность» (information security),
«безопасность ИТ» (IT security),
«сетевая безопасность» (network security),
«безопасность систем» (systems security),
«защита информации» (information protection)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Эволюция понятия (с 1970г.)

«безопасность данных» (англ. data security),
«компьютерная безопасность» (computer security),
«безопасность информации» или «информационная безопасность» (information security),
«безопасность ИТ» (IT security),
«безопасность систем» (systems security) и
«защита информации» (information protection),
«сетевая безопасность» (network security).

Россия:
«безопасность информации» или «информационная безопасность» (information security),
«защита информации» (information protection).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ


ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
БЕЗОПАСНОСТЬ (Б)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

БЕЗОПАСНОСТЬ (Б)

Б - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз (Закон РФ от 05.03.1992 № 2446-1 «О безопасности»)

Угроза - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности … [ГОСТ Р 50922-2006];

Б – … (Закон РФ от 28.12.2010 № 390-ФЗ)

Б – отсутствие недопустимого риска, связанного с возможностью нанесения ущерба (ГОСТ Р 1.1-2002)

Риск – вероятность причинения вреда с учетом его тяжести (Закон РФ № 184-ФЗ «О техническом регулировании»);

Б (защищаемого объекта - предприятие, организация, учреждение, домовладение и т.п.) - состояние защищенности объекта от угроз причинения ущерба (вреда) жизни и здоровью людей, имуществу физических и юридических лиц, государственному и муниципальному имуществу, техническому состоянию, инфраструктуре жизнеобеспечения, внешнему виду, интерьеру(ам), ландшафтной архитектуре, окружающей природной среде (ГОСТ Р 53704-2009 «Системы безопасности комплексные и интегрированные. Общие технические требования»).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

↓

Доктрина информационной безопасности Российской Федерации:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

↓

Доктрина информационной безопасности Российской Федерации:

↓

«Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Доктрина информационной безопасности Российской Федерации:

«Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»

Интересы личности в информационной сфере:
реализация 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 на защиту информации, обеспечивающей личную безопасность

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Доктрина информационной безопасности Российской Федерации:

«Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства»

Интересы личности в информационной сфере:
реализация 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 на защиту информации, обеспечивающей личную безопасность

Интересы государства в информационной сфере:
создание 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, безусловное обеспечение законности и правопорядка, развитие равноправного и взаимовыгодного международного сотрудничества

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

↓

Чаще всего понимают:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Чаще всего понимают:

- *направление научных исследований;*
- *направление образовательной деятельности;*
- *защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры;*
- *механизм защиты, обеспечивающий конфиденциальность, целостность и доступность информации;*
- *свойство информации сохранять конфиденциальность, целостность и доступность;*
- *состояние защищенности*

Информационная безопасность < объекта> **- это состояние защищенности объекта от угроз в информационной сфере.**

Если < объект> : Российская Федерация

ИБ РФ **[Доктрина ИБ РФ] - состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства**

Интересы личности в информационной сфере:
реализация 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 на защиту информации, обеспечивающей личную безопасность
Интересы государства в информационной сфере:
создание 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, безусловное обеспечение законности и правопорядка, развитие равноправного и взаимовыгодного международного сотрудничества

Информационная безопасность < объекта> **- это состояние защищенности объекта от угроз в информационной сфере.**

Если < объект> : организация банковской системы (БС) РФ:

ИБ организации БС РФ **[СТО БР ИББС-1.0] - это безопасность (состояние защищенности интересов (целей) организации БС РФ в условиях угроз), связанная с угрозами в информационной сфере.**

При этом защищенность достигается обеспечением совокупности свойств ИБ — доступности, целостности, конфиденциальности информационных активов, а информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

Информационная безопасность < объекта> **- это состояние защищенности объекта от угроз в информационной сфере.**

Если < объект> : данные, информация или объект информатизации, то

ИБ < объекта>  **Безопасность информации (БИ)**

Безопасность информации [данных] **– это состояние защищенности информации, при котором обеспечивается ее [их] конфиденциальность, доступность и целостность [ГОСТ Р 50922-2006], а также неотказуемость, подотчетность, аутентичность и достоверность**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

↓

Свойства информации:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

↓

Свойства информации:

↓

Конфиденциальность: *доступ к информации только авторизованных пользователей*

Доступность: *доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости*

Целостность: *достоверность и полнота информации и методов ее обработки;*

ГОСТ Р ИСО/МЭК 27002-2012

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Свойства информации:

Конфиденциальность: *доступ к информации только авторизованных пользователей*

Доступность: *доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости*

Целостность: *достоверность и полнота информации и методов ее обработки;*

ГОСТ Р ИСО/МЭК 27002-2012

Аутентичность или подлинность (authenticity) - *свойство, гарантирующее, что субъект или ресурс идентичны заявленным;*

Неотказуемость или неоспоримость (non-repudiation) – *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];

Достоверность или функциональность (reliability) –
свойство соответствия преднамеренному поведению и результатам [ГОСТ Р ИСО/МЭК 13335-1-2006];

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Информационная безопасность < объекта> - это состояние защищенности объекта от угроз в информационной сфере. При этом защищенность достигается обеспечением совокупности свойств ИБ — доступности, целостности, конфиденциальности активов объекта.

Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

- *состояние защищенности объекта от угроз в информационной сфере. При этом защищенность достигается обеспечением совокупности свойств ИБ — доступности, целостности, конфиденциальности активов объекта.*

- *это состояние защищенности информации, при котором обеспечивается ее [их] конфиденциальность, доступность и целостность [ГОСТ Р 50922-2006], а также неотказуемость, подотчетность, аутентичность и достоверность*

Информационная безопасность < объекта> - это состояние защищенности объекта от угроз в информационной сфере.
При этом защищенность достигается обеспечением совокупности свойств ИБ — доступности, целостности, конфиденциальности активов объекта.

Обеспечение информационная безопасности (ОИБ) <объекта> **- это процессы поддержания состояния объекта ИБ;**

Система обеспечения ИБ» (СОИБ) **– это совокупность связанных процессов ОИБ, мер и средств обеспечения ИБ а также необходимых для этого ресурсов.**

ГОСТ Р 50922-2006:

Защита информации **– это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.**

ОИБ = ЗИ

Р. Декарт:
"Дайте понятиям точное толкование, и вы освободите мир от половины заблуждений»

Основы информационной безопасности критически важных объектов

Информационная безопасность

состояние защищенности объекта от угроз в информационной сфере. При этом защищенность достигается обеспечением совокупности свойств ИБ — доступности, целостности, конфиденциальности активов объекта.

Основы (обеспечения) информационной безопасности критически важных объектов

Р. Декарт:
"Дайте понятиям точное толкование, и вы освободите мир от половины заблуждений»

Основы информационной безопасности критически важных объектов

Информационная безопасность

Критически важные объекты

Критически важные объекты

Критически важные объекты

↓

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации

(Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803)

Критически важные объекты

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации

(Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803)

Критически важный объект инфраструктуры Российской Федерации (далее - критически важный объект) - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок

Критически важные объекты

↓

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации

(Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803)

↑

Автоматизированная система управления производственными и технологическими процессами КВО инфраструктуры РФ - комплекс аппаратных и программных средств, информационных систем и информационно- телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса КВО, нарушение (или прекращение) функционирования которых может нанести вред внешнеполитическим интересам РФ, стать причиной аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизации работы учреждений, предприятий или организаций, нанесения материального ущерба в крупном размере, смерти или нанесения тяжкого вреда здоровью хотя бы одного человека и (или) иных тяжелых последствий

Критически важные объекты

↓

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации

(Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803)

↑

Безопасность автоматизированной системы управления КВО - **состояние** автоматизированной системы управления КВО, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения ею целевых функций (далее - штатный режим функционирования) при проведении в отношении ее компьютерных атак;

Компьютерная атака - целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях;

Критически важные объекты

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов

(Приняты Постановление Парламентской Ассамблеи ОДКБ 27.11.2014 года № 7-5):

Государства – члены ОДКБ: Российская Федерация, Республика Белорусь, Республика Казахстан, Республика Таджикистан, Кыргызская Республика, Республика Армения.

Критически важные объекты - объекты социальной, производственной, инженерной, транспортной, энергетической, информационно-коммуникационной и иной инфраструктуры, нарушение функционирования которых в результате акта терроризма, также других негативных воздействий, может оказать влияние на принятие органами власти решений, воспрепятствовать политической или иной общественной деятельности, спровоцировать осложнение международных отношений или войну, устрашить население, дестабилизировать общественный порядок и (или) повлечь за собой человеческие жертвы, причинение вреда здоровью людей или окружающей среде, значительный материальный ущерб и нарушение условий жизнедеятельности людей.

Критически важные объекты

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов

(Приняты Постановление Парламентской Ассамблеи ОДКБ 27.11.2014 года № 7-5):

Государства – члены ОДКБ: Российская Федерация, Республика Белорусь, Республика Казахстан, Республика Таджикистан, Кыргызская Республика, Республика Армения.

Обеспечение безопасности критически важных объектов - реализация определяемой государством-членом ОДКБ системы правовых, экономических, организационных и иных мер, направленных на обеспечение состояния защищенности критически важных объектов.

Критически важные объекты

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов

(Приняты Постановление Парламентской Ассамблеи ОДКБ 27.11.2014 года № 7-5):

Государства – члены ОДКБ: Российская Федерация, Республика Белорусь, Республика Казахстан, Республика Таджикистан, Кыргызская Республика, Республика Армения.

Критические элементы критически важных объектов - зоны, территории, административно-производственные здания и сооружения, конструктивные и технологические элементы критически важного объекта, элементы систем, оборудования или устройств потенциально опасной установки, места использования, хранения и уничтожения опасных веществ и материалов, несанкционированные действия в отношении которых приводят к прекращению нормального функционирования критически важно объекта, его повреждению или аварии, или созданию угрозы возникновения чрезвычайной ситуации.

Критически важные объекты

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации

(Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803)

Критически важный объект инфраструктуры Российской Федерации (далее - критически важный объект) - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок

Критически важные объекты

Критически важный объект — объект, оказывающий существенное влияние на национальную безопасность Российской Федерации, прекращение или нарушение функционирования которого приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, другой сферы хозяйства или инфраструктуры страны, либо для жизнедеятельности населения, проживающего на соответствующей территории, на длительный период времени

Ключевая (критически важная) система информационной инфраструктуры (КСИИ) — информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан и в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация или будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

Критически важные объекты

↓

Ключевая (критически важная) система информационной инфраструктуры (КСИИ)

↓

КСИИ входят в состав:

- ✓ систем органов государственной власти;
- ✓ систем органов управления правоохранительных структур;
- ✓ систем финансово-кредитной и банковской деятельности;
- ✓ систем предупреждения и ликвидации чрезвычайных ситуаций;
- ✓ географические и навигационные систем;
- ✓ сети связи общего пользования на участках, без резервных видов связи;
- ✓ систем специального назначения;
- ✓ спутниковых систем для обеспечения органов управления и в спец. целях;
- ✓ систем управления добычей и транспортировкой нефти, нефтепродуктов и газа;
- ✓ программно-технические комплексов центров управления ВСС;
- ✓ систем управления водоснабжением и энергоснабжением;
- ✓ систем управления транспортом (наземным, воздушным, морским);
- ✓ систем управления потенциально опасными объектами.

Определения других терминов будут даваться в рамках рассмотрения последующих тем из учебного плана дисциплины

Информационные источники:

Рекомендации по гармонизации законодательства государств – членов Организации Договора о коллективной безопасности (ОДКБ) в сфере обеспечения безопасности критически важных объектов (Приняты Постановление Парламентской Ассамблеи ОДКБ 27.11.2014 года № 7-5):

Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере ИБ. . – М.: Горячая линия–Телеком, 2012. – 140 с.
Раздел: Глоссарий основных терминов и определений в области лицензирования и сертификации (стр. 82-128)

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

ГОСТ Р ИСО/МЭК 13335-1-2006. Информационные технологии. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

Справочник терминов по ИБ - http://www.glossary.ib-bank.ru

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