МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра информационной безопасности

НОРМАТИВНЫЕ ДОКУМЕНТЫ И СТАНДАРТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Организация и технологии защиты информации»
(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА
Рабочая программа дисциплины

Составитель:
д.т.н, профессор В.В. Арутюнов

Ответственный редактор
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры
Информационной безопасности
№ 9 от 17.03.2023

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель курса: формирование у обучающихся знаний об отечественных и зарубежных нормативных актах, стандартах и нормативных документах- регуляторов в области обеспечения безопасности информационных систем и сетей.

Задачи курса:

- рассмотреть задачи нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности, структуру и содержание системы нормативного обеспечения безопасности;
- раскрыть вопросы нормативного регулирования развития терминологии в области обеспечения безопасности информационных систем и сетей, нормативного регулирования технической и криптографической защиты информации;
- рассмотреть и освоить обучающимися стандарты в области обеспечения функциональной безопасности информационных систем и сетей, управления информационной безопасностью.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1 Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта ОПК-12.2 Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации ОПК-12.3 Владеет	1) Знать: - терминологию моделирования процессов и систем защиты информации; - основные методы моделирования процессов и систем защиты информации, основные принципы и приемы построения моделей; - основные нормативно-правовые акты, регламентирующие вопросы определения и моделирования угроз безопасности информации в информационных системах; - методологии и средства структурного моделирования процессов и систем. 2) Уметь: - использовать нормативно-правовые акты, регламентирующие вопросы

	навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений	определения и моделирования угроз безопасности информации в информационных системах; - использовать принципы и методы моделирования процессов и систем защиты информации; - использовать методологии и средства моделирования процессов и систем, основные принципы и приемы построения моделей; - анализировать результаты процесса моделирования, формулировать предложения по оптимизации и улучшению функционирования моделируемой системы или процесса. Владеть: - терминологией моделирования процессов и систем защиты информации; - навыками использования правовых и нормативных требований к определению и моделированию угроз безопасности информации в информационных системах; - методологиями и средствами моделирования процессов и систем; - навыками анализа результатов процесса моделирования, формулирования предложений по оптимизации и улучшению функционирования моделируемой системы или процесса.
ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК-2.3.1 Знает национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов	Знать особенности государственно-конституционного устройства и правовые основ современного Российского государства, соотношения прав отдельных личностей, общества и государства в целом, а также характеристики и содержание основных отраслей права; Уметь: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов Владеть: навыками использовать

	исполнительной власти в области внедрения и эксплуатации средств защиты информации ОПК-2.3.2 Умеет документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям ОПК-2.3.3 Владеет навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям	основы правовых знаний в различных сферах деятельности

1.3. Место дисциплины в структуре образовательной программы

Дисциплина (модуль) «Специальные нормативные документы и стандарты по информационной безопасности» относится к базовой части блока дисциплин учебного плана.

Для освоения дисциплины (модуля) необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: Основы информационной безопасности, Правовое обеспечение информационной безопасности, Экономика защиты информации.

В результате освоения дисциплины (модуля) формируются знания, умения и владения, необходимые для прохождения преддипломной практики и подготовки и защиты ВКР и дисциплин: Комплексное обеспечение безопасности объекта информатизации. Управление службой защиты информации, а также Аудит информационной безопасности.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
7	Лекции	**28**
7	Практические занятия	**34**
	Всего:	**62**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 46 академических часов.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
	Тема 1. Основы технического регулирования и стандартизации в Российской Федерации	Предмет и содержание дисциплины, методы изучения, основная литература, контроль освоения дисциплины. Основные термины в области защиты информации. Основная задача стандартов в сфере информационной безопасности. Категории сторон, заинтересованных в создании и развитии стандартов в сфере информационной безопасности. Федеральный закон Российской Федерации "О техническом регулировании". Правила разработки национальных стандартов (ГОСТ Р 1.2-2014).
	Тема 2. Национальные и международные стандарты в	Основные базовые требования к безопасности, впервые сформулированные в "Оранжевой

	области информационной безопасности	книге". Международный стандарт ISO/IEC 15408-99 («Общие критерии»). Национальный стандарт ГОСТ Р ИСО/МЭК 15408—2002 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Международная серия стандартов ISO/IEC 27000. Национальный стандарт по менеджменту инцидентов информационной безопасности ГОСТ Р ИСО/МЭК ТО 184044-2007.
	Тема 3. Национальные стандарты Российской Федерации в области информационной безопасности	Национальный стандарт ГОСТ Р ИСО/МЭК 15408-1-2012. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-2-2012. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-3-2012. Национальные стандарты серии ГОСТ Р 34.10 для криптографической защиты систем обработки информации. Национальные стандарты по биометрической аутентификации серий ГОСТ Р ИСО/МЭК 19784 и ГОСТ Р 52633. Национальные стандарты в сфере управления информационной безопасностью серии ГОСТ Р ИСО/МЭК 27000.
	Тема 4. Нормативные документы ФСТЭК России	Защита от НСД - несанкционированного доступа к информации: термины и определения. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем от НСД к информации. Классификация автоматизированных систем и требования по защите информации. Показатели защищённости межсетевых

		экранов от НСД. Классификация межсетевых экранов по уровню защищённости от несанкционированного доступа к информации. Контроль отсутствия недекларированных возможностей в программном обеспечении.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	2	3	4
1.	Основы технического регулирования и стандартизации в Российской Федерации	Лекция 1 Семинар 1	Вводная лекция с использованием видеопроектора Опрос
2.	Национальные и международные стандарты в области информационной безопасности	Лекция 2 Семинар 2	Лекция с использованием видеопроектора опрос
3.	Национальные стандарты Российской Федерации в области информационной безопасности	Лекция 3 Семинар 3	Лекция с использованием видеопроектора опрос
4.	Нормативные документы ФСТЭК России	Лекция 4 Семинар 4 Контрольная работа 2	Лекция с использованием видеопроектора Опрос Подготовка к контрольной с использованием материалов лекций и литературы

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
- работа на практических занятиях	5 баллов	40 баллов
- контрольная работа	10 баллов	20 баллов
Промежуточная аттестация –зачет (тестирование)		40 баллов
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично/ зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
82-68/ C	хорошо/ зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	удовлетво-рительно/ зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	неудовлет-ворительно/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Текущий контроль (вариант опросного задания)

Вопросы	***Реализуемая компетенция***
1. Базовые органы - генераторы правовых документов в сфере ИБ в России на федеральном уровне	***ОПК-5***
2. Основные категории сторон, заинтересованные в создании и развитии национальных стандартов в сфере информационной безопасности.	***ПК-5***
3. Базовые задачи стандартов в сфере информационной безопасности.	***ПК-10***

4. Объекты информатизации, аттестуемые по требованиям безопасности информации.	***ПСК-2.4***

Примерная тематика контрольной работы - проверка сформированности компетенций ОПК-5, ПК-5, ПК-10, ПСК-2.4

1. Классификация стандартов ИБ.
2. Базовые нормативные документы по техническому регулированию и стандартизации в РФ.
3. Классификация источников норм в стандартизации.
4. Базовые категории сторон, заинтересованные в создании и развитии национальных стандартов в сфере информационной безопасности.
5. Основные группы классификация автоматизированных систем в соответствии с требованиями по защите информации.
6. Базовые этапы разработки национальных стандартов в РФ.
7. Классификация МЭ по уровню контроля отсутствия незадекларированных возможностей.
8. Структура системы стандартов по защите информации.

Промежуточная аттестация (примерные контрольные вопросы по курсу) - проверка сформированности компетенций ОПК-5, ПК-5, ПК-10, ПСК-2.4

1. Основные федеральные органы РФ, формирующие нормативно-правовые документы в области информационной безопасности.
2. Содержание ФЗ "О техническом регулировании".
3. Основные принципы стандартизации в России.
4. Базовые объекты стандартизации в России.
5. Основные правила разработки национальных стандартов в России.
6. Структура стандартов России в области защиты информации.
7. Основные задачи системы стандартизации в России в области защиты информации.
8. Порядок разработки и утверждения стандартов организаций.
9. Базовые этапы разработки стандарта в России.
10. Краткая характеристика международных стандартов серии ISO/IEC 27000.
11. Базовые национальные стандарты России для криптографической защиты систем обработки информации.
12. Классификация автоматизированных систем в соответствии с требованиями по защите информации.
13. Классификация СВТ в соответствии с требованиями по защите информации.

14. Основные требования по защите, предъявляемые к межсетевым экранам.
15. Классификация программного обеспечения по уровню контроля отсутствия недекларированных возможностей.
16. Классификация межсетевых экранов по уровню защищённости от несанкционированного доступа к информации.
17. Основные уровни контроля отсутствия НДВ в программном обеспечении, установленные в РД ФСТЭК России.
18. Основные классы защищенности, установленные для средств антивирусной защиты.
19. Базовые классы защищенности, установленные для средств обнаружения вторжений.
20. Основные классы защищенности, установленные для средств контроля съемных машинных носителей информации.
21. Основные положения документа «Политика информационной безопасности».
22. Этапы работ по защите от угроз, использующих скрытые каналы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

1. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ // СЗ РФ 31.07.2006, N 31 (1 ч.). - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон Российской Федерации от 27.12.2002 г. № 184-ФЗ «О техническом регулировании». «Собрание законодательства РФ», 30.12.2002, № 52 (ч.1), ст. 5140. - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_40241/

Литература

основная

1. Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info

дополнительная

1.Кузнецов И.Н., Бизнес-безопасность. - М.: Дашков и К, 2016. - 416 с. - Режим доступа: URL: http://znanium.com/catalog/product/430343

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ru www.grebennikon.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:
1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security
4. Mozilla Firefox

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

Планы практических занятий

Практическое занятие 1. (Тема 1). Содержание Федерального закона Российской Федерации "О техническом регулировании" - **(2 часа)** - ***проверка сформированности компетенций ОПК-12; ОПК-2.3***

Вопросы для изучения и обсуждения:

1. Базовые органы - генераторы в России на федеральном уровне правовых документов в

сфере ИБ.

2. Цели Федерального закона Российской Федерации "О техническом регулировании".

3. Основные документы в области стандартизации, действующие на территории Российской Федерации после ввода в действие ФЗ "О техническом регулировании".

4. Базовые принципы технического регулирования в России.

Контрольные вопросы:

1. Сущность стандарта и технического регламента.
2. Какие вопросы регулируются ФЗ "О техническом регулировании"?
3. Цели принятия технических регламентов.
4. Порядок разработки и утверждения национальных стандартов.

Список литературы

Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ // СЗ РФ 31.07.2006, N 31 (1 ч.). - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон Российской Федерации от 27.12.2002 г. № 184-ФЗ «О техническом регулировании». «Собрание законодательства РФ», 30.12.2002, № 52 (ч.1), ст. 5140. - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_40241/

Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info

Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru

Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/

Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru

Национальный открытый университет ИНТУИТ - Режим доступа: URL: http://www.intuit.ru

Практическое занятие 2. (Тема 2). Международная серия стандартов ISO/IEC 27000 - **(8 часов) - *проверка сформированности компетенций - ОПК-12; ОПК-2.3***

Вопросы для изучения и обсуждения:

1. Основные причины подготовки и выпуска стандартов серии ISO/IEC 2700.
2. Категории пользователей стандартов серии ISO/IEC 2700.
3. Сферы информационной безопасности, в которой действуют стандарты серии ISO/IEC 27000.
4. Основные кластеры стандартов, выделяемые во множестве стандартов серии ISO/IEC 27000.

5. Национальные стандарты России, гармонизированные со стандартами серии ISO/IEC 27000.

6. Основные разработчики стандартов серии ISO/IEC 27000.

Контрольные вопросы:

1. Какие первые стандарты в сфере ИБ были приняты в мире?

2. По каким признакам классифицируются стандарты серии ISO/IEC 27000?

3. В каком стандарте и каким образом определяется система менеджмента информационной безопасности (СМИБ)?

4. Основные принципы успешной реализации СМИБ.

5. В чём суть процессного подхода для СМИБ «План — Осуществление — Проверка — Действие»?

6. Основные действия организации для разработки СМИБ.

Список литературы

Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info

Кузнецов И.Н., Бизнес-безопасность. - М.: Дашков и К, 2016. - 416 с. - Режим доступа: URL: http://znanium.com/catalog/product/430343

Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru

Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/

Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru

Национальный открытый университет ИНТУИТ - Режим доступа: URL: http://www.intuit.ru

Практическое занятие 3. (Тема 3). Национальные стандарты по биометрической аутентификации серии ГОСТ Р 52633 - **(2 часа)** - ***проверка сформированности компетенций*** - ***ОПК-12; ОПК-2.3***

Вопросы для изучения и обсуждения:

1. Основные области стандартизации, относящиеся к биометрии.
2. Базовые подсистемы биометрической системы защиты информации.
3. Основные функции обобщённой биометрической системы.
4. Формат записи биометрической информации.

Вопросы для изучения и обсуждения:

1. Базовые стандарты серии ГОСТ Р 52633.
2. Основные физиологические и поведенческие биометрические идентификаторы.

3. На основе каких биометрических идентификаторов функционируют современные системы защиты информации?

4. Какое количество национальных стандартов в сфере биометрической защиты информации на начало 2017 г. действует в России и о чём оно свидетельствует?

Список литературы

Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info

Кузнецов И.Н., Бизнес-безопасность. - М.: Дашков и К, 2016. - 416 с. - Режим доступа: URL: http://znanium.com/catalog/product/430343

Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru

Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/

Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru

Национальный открытый университет ИНТУИТ - Режим доступа: URL: http://www.intuit.ru

Практическое занятие 4. (Тема 4). Классификация автоматизированных систем с учётом требований по защите информации - **(2 часа) - *проверка сформированности компетенций* - ОПК-12; ОПК-2.3**

Вопросы для изучения и обсуждения:

1. Основные группы автоматизированных систем с учетом уровня их защищённости.
2. Базовые требования к автоматизированным системам для декомпозиции их на различные классы.
3. Классификация автоматизированных систем с учетом уровня их защищённости.
4. Базовые подсистемы в составе автоматизированной системы 1-го класса защищённости.

Контрольные вопросы:

1. Какие основные стандарты в России посвящены средствам защиты автоматизированных систем?
2. Основные признаки группировки автоматизированных систем в различные классы с учётом уровня защиты в них информации.
3. Базовые группы, на которые декомпозируется в России множество автоматизированных систем с учетом уровня их защищённости.
4. Какие основные подсистемы должна содержать автоматизированная система для обеспечения защиты информации?

Список литературы

Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info

Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru

Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/

Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.

Целью дисциплины (модуля) является формирование у обучающихся знаний об отечественных и зарубежных нормативных актах, стандартах и нормативных документах-регуляторов в области обеспечения безопасности информационных систем и сетей.

Задачи дисциплины:

- рассмотреть задачи нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности, структуру и содержание системы нормативного обеспечения безопасности;
- раскрыть вопросы нормативного регулирования развития терминологии в области обеспечения безопасности информационных систем и сетей, нормативного регулирования технической и криптографической защиты информации;
- рассмотреть и освоить обучающимися стандарты в области обеспечения функциональной безопасности информационных систем и сетей, управления информационной безопасностью.

Дисциплина направлена на формирование следующих компетенций:

ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений

ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта

национальные, межгосударственные и международные стандарты в области защиты информации, нормативные правовые акты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти в области внедрения и эксплуатации средств защиты информации

Уметь:

определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации

документировать процедуры и результаты контроля функционирования системы защиты информации; проводить испытания программно-технических средств защиты информации от НСД и специальных воздействий на соответствие требованиям по безопасности информации и техническим условиям

Владеть:

навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений

навыками внесения изменений в эксплуатационную документацию и организационно-распорядительные документы по системе защиты информации; навыками разработки программ и методик испытаний опытного образца программно-технического средства защиты информации от НСД и специальных воздействий на соответствие техническим условиям

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.
Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.