Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый Проректор
_____ / Т.Р. Змызгова /
«31» августа 2023 г.

Рабочая программа учебной дисциплины

СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем
Специализация: (специализация №5) Безопасность открытых информационных систем

Форма обучения: очная

Курган 2023

Рабочая программа дисциплины «Стандарты информационной безопасности» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Безопасность открытых информационных систем), утвержденным для очной формы обучения « 30 » 06 2022 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 31 августа 2023 года, протокол № 1

Рабочую программу составил:
ст. преподаватель В.В. Москвин

Согласовано:

Заведующий кафедрой «БИАС»
канд. техн. наук, доцент Д.И. Дик

Начальник Управления
образовательной деятельности И.В. Григоренко

Специалист по учебно-методической
работе Учебно-методического
отдела Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		7
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**64**	**64**
Лекции	32	32
Лабораторные работы	-	-
Практические занятия	32	32
Самостоятельная работа, всего часов в том числе:	**44**	**44**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (подготовка к практическим занятиям и рубежному контролю)	26	26
Вид промежуточной аттестации	**зачет с оценкой**	**зачет оценкой**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Стандарты информационной безопасности» относится к дисциплинам части, формируемая участниками образовательных отношений Блока 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

- Основы информационной безопасности.
- Криптографические методы защиты информации.
- Безопасность сетей ЭВМ.
- Безопасность операционных систем.

Результаты обучения по дисциплине необходимы для изучения дисциплины «Аудит информационной безопасности», выполнения разделов курсового проекта по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем», разделов курсовой работы по дисциплине «Управление информационной безопасностью», а также выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины является изучение наиболее важных стандартов и спецификаций в области информационной безопасности.

Задачами дисциплины являются:

- освоение актуальных российских и международных стандартов и спецификаций ИБ;
- изучение принципов и порядка использования этих стандартов и спецификаций.

Компетенции, формируемые в результате освоения дисциплины:

- способен подготавливать и оформлять научно-технические отчеты, публиковать результаты выполненной работы (ПК-2);
- способность оценивать соответствия механизмов безопасности открытых информационных систем требованиям существующих нормативных документов (ПК-9);

В результате изучения дисциплины обучающийся должен:

знать:

- основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; (для ПК-9);

уметь:

- анализировать и оценивать угрозы информационной безопасности объекта (для ПК-2, ПК-9);
- применять требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации (для ПК-2, ПК-9).

владеть:

- методами оценки информационных рисков (для ПК-2, ПК-9);

- навыками применения различных методов и мер обеспечения доверия к информационной безопасности: лицензирование, аккредитация, оценка и подтверждение соответствия (для ПК-2, ПК-9).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Практич. занятия	Лаборатор. работы
Рубеж 1	1	Обзор наиболее важных стандартов и спецификаций в области информационной безопасности.	1	-	-
	2	«Общие критерии». Основные идеи, функциональные требования безопасности, требования доверия безопасности.	5	6	-
	3	Профили защиты, разработанные на основе «Общих критериев». Общие и частные требования к сервисам безопасности, частные требования к комбинациям и приложениям сервисов безопасности.	6	6	-
	4	Рекомендации семейства X.500	2	-	-
Рубеж 2	5	Спецификации Internet-сообщества	12	12	-
	6	Британский стандарт BS 7799 (ISO/IEC 17799:2005).	2	3	-
	7	Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей».	2	5	-
	8	Основы сертификации средств защиты информации	2	-	-
		Всего:	**32**	**32**	-

4.2. Содержание лекционных занятий

Тема 1. Обзор наиболее важных стандартов и спецификаций в области информационной безопасности.

Роль стандартов и спецификаций. Наиболее важные стандарты и спецификации в области информационной безопасности. Краткие сведения о стандартах и спецификациях, не являющихся предметом данного курса. Краткие аннотации подробно рассматриваемых в курсе стандартов и спецификаций.

Тема 2. «Общие критерии». Основные идеи, функциональные требования безопасности, требования доверия безопасности.

История создания и текущий статус «Общих критериев». Основные понятия и идеи «Общих критериев». Основные понятия и идеи «Общей методологии оценки безопасности информационных технологий».

Классификация функциональных требований безопасности. Классы функциональных требований, описывающие элементарные сервисы безопасности. Классы функциональных требований, описывающие производные сервисы безопасности. Защита данных пользователя. Защита функций безопасности объекта оценки. Классы функциональных требований, играющие инфраструктурную роль.

Основные понятия и классификация требований доверия безопасности. Оценка профилей защиты и заданий по безопасности. Требования доверия к этапу разработки. Требования к этапу получения, представления и анализа результатов разработки. Требования к поставке и эксплуатации, поддержка доверия. Оценочные уровни доверия безопасности.

Тема 3. Профили защиты, разработанные на основе «Общих критериев». Общие и частные требования к сервисам безопасности, частные требования к комбинациям и приложениям сервисов безопасности.

Общие положения. Общие предположения безопасности. Общие угрозы безопасности. Общие элементы политики и цели безопасности. Общие функциональные требования. Общие требования доверия безопасности.

Биометрическая идентификация и аутентификация. Требования к произвольному (дискреционному) управлению доступом. Требования к принудительному (мандатному) управлению доступом. Ролевое управление доступом. Межсетевое экранирование. Системы активного аудита. Анонимизаторы. Анализ защищенности.

Операционные системы. Виртуальные частные сети. Виртуальные локальные сети. Смарт-карты. Некоторые выводы.

Тема 4. Рекомендации семейства X.500.

Основные понятия и идеи рекомендаций семейства X.500. Каркас сертификатов открытых ключей. Каркас сертификатов атрибутов. Простая и сильная аутентификация.

Тема 5. Спецификации Internet-сообщества.

Архитектура средств безопасности IP-уровня. Контексты безопасности и управление ключами. Протокольные контексты и политика безопасности. Обеспечение аутентичности IP-пакетов. Обеспечение конфиденциальности сетевого трафика.

Основные идеи и понятия протокола TLS. Протокол передачи записей. Протокол установления соединений и ассоциированные протоколы. Применение протокола HTTP над TLS. «Обобщенный прикладной программный интерфейс службы безопасности».

Введение. Основные понятия. Функции для работы с удостоверениями. Создание и уничтожение контекстов безопасности. Защита сообщений. Логика работы пользователей интерфейса безопасности. Представление некоторых объектов интерфейса безопасности в среде языка С.

«Руководство по информационной безопасности предприятия». Основные понятия. Проблемы, с которыми может столкнуться организация. Основы предлагаемого подхода. Общие принципы выработки официальной политики предприятия в области информационной безопасности. Анализ рисков,

идентификация активов и угроз. Регламентация использования ресурсов. Реагирование на нарушения политики безопасности (административный уровень). Подход к выработке процедур для предупреждения нарушений безопасности. Выбор регуляторов для практичной защиты. Ресурсы для предупреждения нарушений безопасности. Реагирование на нарушения безопасности (процедурный уровень).

«Как реагировать на нарушения информационной безопасности». Основные понятия. Взаимодействие между группой реагирования, опекаемым сообществом и другими группами. Порядок публикации правил и процедур деятельности групп реагирования. Описание правил группы реагирования. Описание услуг группы реагирования.

«Как выбирать поставщика Интернет-услуг». Общие положения. Роль поставщика Internet-услуг в реагировании на нарушения безопасности. Меры по защите Internet-сообщества. Маршрутизация, фильтрация и ограничение вещания. Защита системной инфраструктуры. Размещение Web-серверов.

Возможные вопросы к поставщику Internet-услуг.

Тема 6. Британский стандарт BS 7799 (ISO/IEC 17799:2005).

Обзор стандарта BS 7799. Регуляторы безопасности и реализуемые ими цели. Часть 1. Регуляторы общего характера. Регуляторы безопасности и реализуемые ими цели. Часть 2. Регуляторы технического характера. Регуляторы безопасности и реализуемые ими цели. Часть 3. Разработка и сопровождение, управление бесперебойной работой, контроль соответствия. Четырехфазная модель процесса управления информационной безопасностью.

Тема 7. Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей».

Основные понятия и идеи стандарта FIPS 140-2. Требования безопасности. Часть 1. Спецификация, порты и интерфейсы, роли, сервисы и аутентификация. Требования безопасности. Часть 2. Модель в виде конечного автомата, физическая безопасность. Требования безопасности. Часть 3. Эксплуатационное окружение, управление криптографическими ключами. Требования безопасности. Часть 4. Самотестирование, доверие проектированию, сдерживание прочих атак, другие рекомендации.

Тема 8. Основы сертификации средств защиты информации.

Федеральный закон от 27.12.2002г. № 184-ФЗ «О техническом регулировании». Основные цели соответствия продукции, процессов, проектирования, производства техническим регламентом. Понятие сертификата соответствия. Декларация соответствия. Обязательный сертификат. Добровольная сертификация. Положение о сертификации средств защиты информации по требованиям безопасности информации. Перечень средств защиты подлежащих обязательной сертификации. Система сертификации средств защиты подлежащих обязательной сертификации. Признаки отличия систем сертификации.

4.3 Практические занятия

Номер темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
2	«Общие критерии». Основные идеи, функциональные требования безопасности, требования доверия безопасности.	*Практическая работа №1.* «Общие критерии». Основные идеи.	4
		Практическая работа №2. Критерии и методология оценки безопасности информационных технологий.	2
3	Профили защиты, разработанные на основе «Общих критериев». Общие и частные требования к сервисам безопасности, частные требования к комбинациям и приложениям сервисов безопасности.	*Практическая работа №3.* ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования.	2
		Практическая работа №4. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.	2
	1-ый рубежный контроль	***Тестирование***	***2***
5	Спецификации Internet-сообщества.	*Практическая работа №5.* Спецификация Internet-сообщества «Как реагировать на нарушения информационной безопасности» RFC-2350.	4
		Практическая работа №6. Концепция обеспечения информационной безопасности предприятия.	4
		Практическая работа №7. Спецификация Internet-сообщества "Как выбирать поставщика Интернет-услуг" RFC 2196	4
6	Британский стандарт BS 7799.	*Практическая работа №8.* Введение в системы управления защитой информации и BS 7779. Внедрение системы управления защитой информации на соответствие требованиям BS 7799. Внутренний аудит. Системы управления защитой информации на соответствие требованиям BS 7799.	3
7	Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей».	*Практическая работа №9.* Криптографические модули для защиты информации ограниченного доступа.	3
	2-ой рубежный контроль	***Тестирование***	***2***
		Итого:	**32**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей практической работы.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения практических работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале практической работы.

Преподавателем запланировано применение на практических занятиях технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к практическим занятиям, к рубежным контролям и подготовку к зачету с оценкой.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела:	**4**
Обзор наиболее важных стандартов и спецификаций в области информационной безопасности.	0,1
«Общие критерии». Основные идеи, функциональные требования безопасности, требования доверия безопасности	0,5
Профили защиты, разработанные на основе «Общих критериев». Общие и частные требования к сервисам безопасности, частные требования к комбинациям и приложениям сервисов безопасности	1,0
Рекомендации семейства X.500	0,1
Спецификации Internet-сообщества	2,0
Британский стандарт BS 7799 (ISO/IEC 17799:2005).	0,1
Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей».	0,1

Основы сертификации средств защиты информации	0,1
Подготовка к практическим занятиям (по 2 часа на каждое)	18
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4
Подготовка к зачету с оценкой	18
Всего:	**44**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ.
2. Отчеты по практическим занятиям.
3. Банк тестовых заданий к рубежным контролям № 1, № 2.
5. Вопросы к зачету с оценкой.

6.2. Система балльно-рейтинговой оценки работы, обучающихся по дисциплине

№	Наименование	Содержание					
1	Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения обучающихся на первом учебном занятии)*	Распределение баллов					
		Вид учебной работы:	Посещение лекций	Выполнение практической работы	Рубежный контроль №1	Рубежный контроль №2	Зачет с оценкой
		Балльная оценка:	$1_б$ x 16=$16_б$	$5_б$ x 9 =$45_б$	4	5	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и экзамене	60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 74… 90 – хорошо; 91…100 – отлично					

3	Критерии допуска к промежуточной аттестации, возможности получения автоматической экзаменационной оценки по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации по дисциплине за семестр обучающийся должен набрать по итогам текущего и рубежного контроля не менее 51 баллов. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается. Для получения зачета с оценкой без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежного контролей. При этом, на усмотрение преподавателя, бальная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность. Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог бальной оценки по дисциплине не снижается. За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30. Основанием для получения дополнительных баллов являются: - выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем; - участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету с оценкой) набрана сумма менее 51 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает с обучающимися основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий

состоят для 1 и 2 рубежного контроля из 15 вопросов. На каждое тестирование при рубежном контроле обучающемуся отводится 2 академических часа.

Баллы обучающемуся выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%
«удовлетворительно» – 50% - 70%
«хорошо» – 70% - 90%
«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого обучающегося по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет с оценкой проводится в традиционной форме. Билет состоит из 2 вопросов. Вопросы к зачету доводятся до обучающихся на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа обучающемуся отводится 1 астрономический час.

Результаты текущего контроля успеваемости и зачета заносятся преподавателем в экзаменационную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку обучающегося.

6.4. Примеры оценочных средств для рубежных контролей и зачета

1-ый рубежный контроль

1. Согласно версии 2.1 «Общих критериев», уровень протоколирования может быть …

а) пониженным
б) базовым
в) повышенным

2. Согласно версии 2.1 «Общих критериев», в число семейств класса «приватность» входят:

а) не регистрируемость
б) невозможность именования
в) невозможность ассоциации

3. Требования «Общих критериев» группируются в

а) семейства б) подсемейства в) подгруппы

4. Согласно «Общим критериям», стойкость функции безопасности может быть…

а) низкой б) умеренной в) высокой

5. Рекомендации X.509 регламентируют следующие аспекты:

а) каркас сертификатов открытых ключей
б) каркас генерации открытых и секретных ключей
в) каркас управления криптографическими ключами

2-ой рубежный контроль

1. Согласно спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности", группа реагирования обязана:

а) предоставлять доверенный канал для приема сообщений о предполагаемых нарушениях

б) снабдить опекаемое сообщество криптографическими средствами

в) выполнять для опекаемого сообщества роль удостоверяющего центра

2. Согласно спецификации Internet-сообщества «Как выбирать поставщика Интернет Internet-услуг», регистрационная информация о системах поставщика должна быть доступна:

а) на чтение и запись всем пользователям

б) на чтение всем пользователям

в) на чтение только системному администратору

3. Согласно стандарту BS 7799, меры по безопасному администрированию систем и сетей разбиты на следующие подгруппы:

а) безопасное управление паролями

б) безопасное управление носителями

в) безопасное управление доступом

4. В стандарте FIPS 140-2 фигурируют следующие группы требований безопасности:

а) управление доступом

б) роли, сервисы и аутентификация

в) физическая безопасность

5. Спецификация Internet-сообщества «Руководство по информационной безопасности предприятия» описывает меры следующих уровней информационной безопасности:

а) административного

б) процедурного

в) программно-технического

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Роль стандартов и спецификаций.
2. История создания и текущий статус «Общих критериев».
3. Основные понятия и идеи «Общих критериев».
4. Классификация функциональных требований безопасности.
5. Классы функциональных требований, описывающие элементарные сервисы безопасности.
6. Классы функциональных требований, описывающие производные сервисы безопасности.
7. Защита данных пользователя. Защита функций безопасности объекта оценки.
8. Классы функциональных требований, играющие инфраструктурную роль.
9. Основные понятия и классификация требований доверия безопасности.
10. Оценка профилей защиты и заданий по безопасности.
11. Требования доверия к этапу разработки.

12. Требования к этапу получения, представления и анализа результатов разработки.

13. Требования к поставке и эксплуатации, поддержка доверия.

14. Оценочные уровни доверия безопасности.

15. Общие угрозы безопасности. Общие элементы политики и цели безопасности.

16. Общие функциональные требования. Общие требования доверия безопасности.

17. Биометрическая идентификация и аутентификация.

18. Требования к произвольному (дискреционному) управлению доступом.

19. Требования к принудительному (мандатному) управлению доступом.

20. Ролевое управление доступом.

21. Межсетевое экранирование.

22. Системы активного аудита.

23. Анонимизаторы. Анализ защищенности.

24. Операционные системы.

25. Виртуальные частные сети. Виртуальные локальные сети.

26. Смарт-карты.

27. Основные понятия и идеи рекомендаций семейства X.500.

28. Каркас сертификатов открытых ключей. Каркас сертификатов атрибутов.

29. Архитектура средств безопасности IP-уровня.

30. Контексты безопасности и управление ключами.

31. Протокольные контексты и политика безопасности.

32. Обеспечение аутентичности IP-пакетов.

33. Обеспечение конфиденциальности сетевого трафика.

34. Основные идеи и понятия протокола TLS.

35. Протокол передачи записей.

36. Протокол установления соединений и ассоциированные протоколы.

37. Применение протокола HTTP над TLS.

38. «Обобщенный прикладной программный интерфейс службы безопасности».

39. Создание и уничтожение контекстов безопасности. Защита сообщений.

40. «Руководство по информационной безопасности предприятия». Основные понятия.

41. Анализ рисков, идентификация активов и угроз.

42. Регламентация использования ресурсов.

43. Подход к выработке процедур для предупреждения нарушений безопасности.

44. Выбор регуляторов для практичной защиты.

45. Ресурсы для предупреждения нарушений безопасности.

46. Реагирование на нарушения безопасности (процедурный уровень).

47. «Как реагировать на нарушения информационной безопасности». Основные понятия.

48. «Как выбирать поставщика Интернет-услуг». Общие положения.

49. Роль поставщика Internet-услуг в реагировании на нарушения безопасности.

50. Меры по защите Internet-сообщества. Маршрутизация, фильтрация и ограничение вещания.

51. Защита системной инфраструктуры. Размещение Web-серверов.

52. Обзор стандарта BS 7799. Регуляторы безопасности и реализуемые ими цели.

53. Основные понятия и идеи стандарта FIPS 140-2. Требования безопасности.

54. Основы сертификации средств защиты информации.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Галатенко В.А. Стандарты информационной безопасности: курс лекций / [Электронный ресурс]. — М.: НОУ Интуит, 2016. - 308с. ISBN 5-9556-0053-1. - Доступ ЭБС «Консультант студента».

2. Галатенко В.А. Основы информационной безопасности. / [Электронный ресурс]. - М.: Национальный Открытый Университет "ИНТУИТ", 2016 - 208 с. ISBN 5-9556-0052-3. - Доступ ЭБС «Консультант студента».

3. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель ГОСТ Р ИСО/МЭК 15408-1-2012 М.: Стандартинформ, 2013.

4. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности ГОСТ Р ИСО/МЭК 15408-2-2013 М.: Стандартинформ, 2014.

7.2 Дополнительная учебная литература:

1. Гостехкомиссия России. РД. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Москва, 1992.

2. Гостехкомиссия России. РД. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. – Москва, 2002.

3. Британский стандарт BS 7799.

4. Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей».

7.3 Методическая литература:

1. Методические указания для подготовки к практическим занятиям (семинарам) по дисциплине «Стандарты информационной безопасности» для студентов очной формы обучения направлений 10.05.03 и 10.03.01.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Международная организация по стандартизации -https://www.iso.org/;
2. Электронный фонд правовой и нормативно-технической документации - http://docs.cntd.ru;
3. ЭБС «Лань» - https://e.lanbook.com/;
4. ЭБС «Znanium» - https://znanium.com/;
5. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
6. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;
7. Вебинары компании «Код безопасности» - https://www.securitycode.ru/company/events/
8. Аудит информационной безопасности: Читальный зал / Информационный онлайн портал ISO27000.ru - http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti.

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально- техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений,

обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Стандарты информационной безопасности»

образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Специальность: (специализация №5)

Безопасность открытых информационных систем

Трудоемкость дисциплины: 3 з.е. (108 академических часа)

Семестр: 7 (очная форма обучения)

Форма промежуточной аттестации: зачет с оценкой

Содержание дисциплины. Основные разделы.

Обзор наиболее важных стандартов и спецификаций в области информационной безопасности. «Общие критерии». Основные идеи. Функциональные требования безопасности. Требования доверия безопасности. Профили защиты, разработанные на основе «Общих критериев». Общие требования к сервисам безопасности. Частные требования к сервисам безопасности. Частные требования к комбинациям и приложениям сервисов безопасности. Рекомендации семейства X.500. Спецификация Internet-сообщества IPsec. Спецификация Internet-сообщества TLS. Спецификация Internet-сообщества «Обобщенный прикладной программный интерфейс службы безопасности». Спецификация Internet-сообщества. Британский стандарт BS 7799. Федеральный стандарт США FIPS 140-2 «Требования безопасности для криптографических модулей». Основы сертификации средств защиты информации.