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 /
«30» августа 2021 г.

Рабочая программа учебной дисциплины

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем

Специализация: (специализация№5) безопасность открытых информационных систем

Форма обучения: очная

Курган 2021

Рабочая программа дисциплины «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (безопасность открытых информационных систем), утвержденным для очной формы обучения «30» августа 2021 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 29 сентября 2021 года, протокол № 2.

Рабочую программу составил:
канд. тех. наук, доцент Д.И. Дик

Согласовано:

Зав. кафедрой «БИАС»
канд. тех. наук, доцент Д.И. Дик

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

Начальник Управления образовательной деятельности С.Н. Синицын

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часов)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		11
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 экзамену	27	27
Другие виды самостоятельной работы (подготовка к практическим занятиям и рубежному контролю)	17	17
Вид промежуточной аттестации	**экзамен**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» относится к дисциплинам вариативной части, формируемой участниками образовательных отношений, Блока 1, формируемой участниками образовательных отношений.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении дисциплин «Теоретические основы компьютерной безопасности», «Методы проектирования защищённых распределённых информационных систем» «Организационное и правовое обеспечение информационной безопасности» и «Управление информационной безопасностью».

В свою очередь, данная дисциплина обеспечивает подготовку выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Учебная дисциплина «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» реализует требования федерального государственного образовательного стандарта высшего профессионального образования и является важной составляющей профессиональной подготовки специалистов в области обеспечения информационной безопасности.

Целью преподавания дисциплины «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» является освоение основных понятий КИИ, построение моделей угроз и определение средств противодействия им.

Задачами дисциплины являются:

- анализ угроз безопасности информации в значимом объекте КИИ и последствия от их реализации;
- разработка предложений по совершенствованию организационно-распорядительных документов по безопасности значимых объектов КИИ;
- контроль за обеспечением безопасности значимого объекта КИИ

Компетенции, формируемые в результате освоения дисциплины:

- способность обрабатывать и анализировать научно-техническую информации и результаты исследований (ПК-1);
- способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-5).

В результате изучения дисциплины обучающийся должен

знать:

- нормативно правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов КИИ (для ПК-1);
- основные понятия в области обеспечения безопасности информации, обрабатываемой объектами КИИ (для ПК-1);

- принципы организации систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования (для ПК-5);

- процедуру категорирования объектов КИИ, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов КИИ (для ПК-1);

- процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом КИИ (для ПК-5);

- требования к организационным и техническим мерам, к программным и программно-аппаратным средствам, принимаемым для обеспечения безопасности значимых объектов КИИ (для ПК-5);

уметь:

- определять категории значимости объектов КИИ (для ПК-1);

- выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ, возможных способов реализации угроз безопасности и последствий от их реализации (для ПК-1, ПК-5);

- обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ (для ПК-5);

- определять требования к обеспечению безопасности значимого объекта КИИ (для ПК-5);

владеть:

- навыками работы с нормативно правовыми актами, методическими документами в области обеспечения безопасности значимых объектов КИИ (для ПК-1);

- навыками выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта КИИ (для ПК-1, ПК-5);

- навыками проведения работ по контролю состояния безопасности объектов КИИ (для ПК-5).

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	Правовые основы обеспечения безопасности КИИ Российской Федерации.	6	-	-
	2	Угрозы безопасности информации, обрабатываемой на объектах КИИ.	6	10	-
	3	Категорирование объектов КИИ.	8	6	-

	Рубежный контроль №1		-	2	-
Рубеж 2	4	Требования по обеспечению безопасности значимых объектов КИИ.	6	12	-
	5	Система безопасности объекта КИИ.	6	-	-
	Рубежный контроль №2		-	2	-
		Всего:	32	32	-

4.2. Содержание лекционных занятий

Тема 1. Правовые основы обеспечения безопасности КИИ Российской Федерации.

Понятия КИИ, Объекты и субъекты КИИ. Права и обязанности субъектов КИИ. Особенности обеспечения безопасности объектов КИИ Российской Федерации. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ. Основные понятия, термины и определения в области обеспечения безопасности КИИ. Государственный контроль в области обеспечения безопасности значимых объектов КИИ. Цели государственного контроля в области обеспечения безопасности значимых объектов КИИ. Виды и периодичность государственного контроля. Основание для проведения плановых и внеплановых проверок. Система нормативно правовых актов по вопросам обеспечения безопасности КИИ Российской Федерации. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации. Организационно-правовые основы лицензирования деятельности в области защиты информации, аттестации объектов информатизации по требованиям безопасности КИИ Российской Федерации.

Тема № 2. Угрозы безопасности информации, обрабатываемой на объектах КИИ.

Объекты КИИ. Объекты защиты. Понятие и классификация угроз безопасности информации и категорий нарушителей в отношении значимых объектов КИИ. Модель угроз безопасности информации значимого объекта КИИ. Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Типовые компьютерные инциденты для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления. Оценка возможных последствий реализации угроз безопасности значимого объекта КИИ.

Тема 3. Категорирование объектов КИИ.

Правила и порядок категорирования объектов КИИ, сроки направления сведений о результатах категорирования объекта КИИ в ФСТЭК России. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ. Формирование комиссии по категорированию объектов КИИ Российской Федерации. Определение объектов КИИ Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов. Анализ возможных действий нарушителей в отношении объектов КИИ. Анализ угроз безопасности

информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на объекте КИИ. Оценка возможных последствий компьютерных инцидентов на объектах КИИ. Присвоение объектам КИИ Российской Федерации одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости. Подготовка необходимых документов в рамках категорирования объектов КИИ Российской Федерации.

Тема № 4. Требования по обеспечению безопасности значимых объектов КИИ.

Установление требований по обеспечению безопасности значимого объекта КИИ. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ. Планирование, разработка и совершенствование мероприятий по обеспечению безопасности значимого объекта КИИ. Сущность, цели и задачи планирования. Порядок разработки, согласования и утверждения плана мероприятий по обеспечению безопасности значимого объекта КИИ. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ.

Тема № 5. Система безопасности объекта КИИ.

Цели и задачи системы безопасности объекта КИИ. Требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования. Требования к силам обеспечения безопасности значимых объектов КИИ. Требования к организационно-распорядительным документам по безопасности значимых объектов КИИ. Структура системы безопасности значимого объекта КИИ. Подготовка необходимых документов в рамках создания систем безопасности значимых объектов КИИ Российской Федерации и обеспечения их функционирования.

4.3 Практические занятия

Номер темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
2	Угрозы безопасности информации, обрабатываемой на объектах КИИ	*Практическая работа №1.* Анализ угроз безопасности информации и уязвимостей программного обеспечения значимого объекта КИИ с помощью банка данных угроз безопасности информации	4
		Практическая работа №2. Разработка модели угроз безопасности информации значимого объекта КИИ	6
3	Категорирование объектов КИИ	*Практическая работа №3.* Определение значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов	4

		Практическая работа №4. Формирование акта комиссии по категорированию значимого объекта КИИ	2
	Рубежный контроль № 1		2
4	Требования по обеспечению безопасности значимых объектов КИИ	*Практическая работа №5* Разработка плана мероприятий по обеспечению безопасности значимого объекта КИИ	2
		Практическая работа № 6 Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ	6
		Практическая работа №7. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ	4
	Рубежный контроль № 2		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, рубежным контролям и экзамену.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела	***8***
Правовые основы обеспечения безопасности КИИ Российской Федерации.	1
Угрозы безопасности информации, обрабатываемой на объектах КИИ.	2
Категорирование объектов КИИ.	2
Требования по обеспечению безопасности значимых объектов КИИ.	2
Система безопасности объекта КИИ.	1
Подготовка к практическим занятиям (по 0,5 часу на занятие)	7
Подготовка к рубежным контролям (по 1 часу на каждый)	2
Подготовка к экзамену	27
Всего:	***44***

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Отчеты студентов по практическим работам.
3. Задания к рубежным контролям № 1, № 2.
4. Вопросы к экзамену.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание						
1	Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	Распределение баллов						
		Вид учебной работы:	Посещение лекций	Выполнение лабораторных работ	Выполнение практической работы	Рубежный контроль №1	Рубежный контроль №2	Экзамен
		Балльная оценка:	$1,5_б$ x16=$24_б$	-	$4_б$ x 7 =$28_б$	9	9	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и экзамена	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 «автоматом» экзамена по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (экзамену) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все практические работы. Для получения экзаменационной оценки «удовлетворительно» «автоматически» студенту необходимо набрать 68 баллов. По согласованию с преподавателем студенту, набравшему минимум 68 балл, могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена за экзамен «автоматически» оценка «хорошо» или «отлично».
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (экзамену) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических работ. Формы дополнительных заданий (назначаются преподавателем): выполнение и защита пропущенной практической работы (при невозможности дополнительного проведения практической работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 4 баллов. 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 тестирования. Перед проведением рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Тесты состоят из 9 вопросов по 1 баллу каждый. На каждый рубежный контроль студенту отводится 2 академических часа.

Преподаватель оценивает в баллах результаты рубежных контролей каждого студента и заносит в ведомость учета текущей успеваемости.

Баллы студенту 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% .

Экзамен проводится в традиционной форме, по билетам. Билет состоит из 2 вопросов. Вопросы к экзамену доводятся до студентов на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа студенту отводится 1 астрономический час.

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

6.4. Примеры оценочных средств для рубежных контролей и экзамена

1-ый рубежный контроль

1) Типы объектов КИИ:

а) Информационные системы и информационно-телекоммуникационные сети;

б) Автоматизированные системы управления;

в) Информационные системы и автоматизированные системы управления;

г) Информационные системы и Информационно-телекоммуникационные сети и автоматизированные системы управления.

2)Соотнесите права, общие обязанности субъектов КИИ и обязанности субъектов КИИ, имеющие значимые объекты КИИ:

Права субъектов КИИ	Общие обязанности субъектов КИИ	Обязанности субъектов КИИ, имеющие значимые объекты КИИ

а) получение информации о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения;

б) выполнение предписаний об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта КИИ, выданные должностными лицами ФСТЭК России в соответствии со своими компетенциями;

в) приобретение, аренда, установка и обслуживание средств за свой счет, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

г) информирование ФСБ России о компьютерных инцидентах;

д) реагирование на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ в порядке, утвержденном ФСБ России;

е) оказание помощи в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий их возникновения, должностным лицам ФСБ России;

ж) получение информации от ФСТЭК России, необходимой для обеспечения безопасности значимых объектов КИИ, в том числе об угрозах безопасности обрабатываемой информации и уязвимостях программного обеспечения, оборудования и технологий;

з) обеспечение выполнения порядка, технических условий, установки, эксплуатации и сохранность средств ГОССОПКА,

и) соблюдение требования по обеспечению безопасности значимых объектов КИИ, установленных ФСТЭК России;

к) разработка и проведение мероприятий по обеспечению безопасности значимого объекта КИИ;

л) обеспечение беспрепятственного доступа к значимым объектам КИИ при реализации полномочий по осуществлению государственного контроля должностных лиц ФСТЭК России.

3)С какой периодичности проводятся плановые проверки?

а) Раз в год со дня осуществления последней проверки или по мере возникновения компьютерных инцидентов;

б) Раз в 3 года со дня осуществления последней проверки или по мере возникновения компьютерных инцидентов;

в) Раз в 3 года со дня осуществления последней проверки или при истечении срока выполнения предписание на устранение выявленного нарушения требований по обеспечению безопасности;

г) Раз в год со дня осуществления последней проверки или при истечении срока выполнения предписание на устранение выявленного нарушения требований по обеспечению безопасности;

д) По мере возникновения компьютерного инцидента;

е) Раз в год со дня осуществления последней проверки;

ж) Раз в 3 года со дня осуществления последней проверки.

4)Распределите проводимые мероприятия по этапам оценки угроз безопасности информации:

Определение негативных последствий	Определение возможных объектов воздействия	Оценка возможности реализации угроз безопасности информации

а) Источники угроз;

б) Инвентаризация систем и сетей;

в) Анализ документации систем и сетей;

г) Актуальность угроз;

д) Информационные ресурсы и компоненты систем и сетей;

е) Шаблоны атак из открытых источников;

ж) Негативные последствия от реализации угроз;

з) Способы реализации угроз.

5)Местами возникновения уязвимостей в ИС являются:

а) Код;

б) Специальное программное обеспечение;

в) Архитектура;

г) Конфигурации;

д) Сетевое оборудование.

6)Укажите правильный порядок категорирования объектов КИИ:

а) составление акта категорирования, получение исходных данных, сбор комиссии, определение перечня объектов, Отправка перечня объектов во ФСТЭК, категорирование объектов, отправка сведений о результатах;

б) получение исходных данных, определение перечня объектов, Отправка перечня объектов во ФСТЭК, сбор комиссии, категорирование объектов, составление акта категорирования, отправка сведений о результатах;

в) сбор комиссии, получение исходных данных, определение перечня объектов, категорирование объектов, отправка перечня объектов во ФСТЭК составление акта категорирования, отправка сведений о результатах;

г) сбор комиссии, определение перечня объектов, получение исходных данных, Отправка перечня объектов во ФСТЭК, категорирование объектов, составление акта категорирования, отправка сведений о результатах;

д) получение исходных данных, сбор комиссии, определение перечня объектов, составление акта категорирования, Отправка перечня объектов во ФСТЭК, категорирование объектов, отправка сведений о результатах;

е) определение перечня объектов, получение исходных данных, сбор комиссии, Отправка перечня объектов во ФСТЭК, составление акта категорирования, категорирование объектов, отправка сведений о результатах;

ж) получение исходных данных, определение перечня объектов, категорирование объектов, Отправка перечня объектов во ФСТЭК, сбор комиссии, составление акта категорирования, отправка сведений о результатах.

7)На какой срок устанавливается категория значимости объекта КИИ?

а) 1 год;

б) 3 года;

в) 5 лет;

г) 10 лет.

8)Кто занимается категорированием общей, для филиальной сети и компании или её части, системы, которая является объектом КИИ?

а) Владелец системы;

б) Пользователь системы;

в) Устанавливается договором;

г) Уточняются личным обращением во ФСТЭК;

д) Всеми субъектами КИИ, имеющими доступ к системе.

9) Когда разрабатывается модель угроз и нарушителей для объекта КИИ?

а) Непосредственно на этапе категорирования объекта КИИ;

б) После категорирования объекта и присвоения категории значимости;

в) После категорирования объекта, до присвоения категории значимости;

г) На этапе определения перечня объектов КИИ;

д) На этапе присвоения значимости объекта КИИ.

2-ой рубежный контроль

1)К разработке организационных и технических мер защиты значимых объектов КИИ относятся:

а) Моделирование угроз;

б) Разработка документов по безопасности объекта;

в) Выявление уязвимостей;

г) Проектирование системы безопасности;

д) Установка средств защиты;

г) Не проводится.

2)В информационных системах объектами защиты являются:

а) программно-аппаратные средства;

б) информация, передаваемая по линиям связи;

в) средства защиты информации;

г) архитектура и конфигурация ИТС;

д) телекоммуникационное оборудование.

3)В информационно-телекоммуникационных сетях объектами защиты являются:

а) программно-аппаратные средства;

б) средства защиты информации;

в) телекоммуникационное оборудование;

г) программные средства;

д) информация о параметрах управляемого объекта или процесса.

4)В автоматизированных системах управления объектами защиты являются:

а) программно-аппаратные средства;

б) информация, передаваемая по линиям связи;

в) телекоммуникационное оборудование;

г) программные средства;

д) информация о параметрах управляемого объекта или процесса.

5)Выберите выполняемые задачи системы безопасности значимых объектов КИИ:

а) Оценка и анализ попыток неправомерного доступа к информации;

б) Ограничение воздействия на технические средства обработки информации;

в) Защита от НСД к информации;

г) Создание резервных копий объектов и данных;

д) Предотвращение неправомерного доступа у информации;

е) Восстановление работоспособности объектов.

6) Кем определяется состав и формы документов по системе безопасности ЗОКИИ?

а) Указаниями ФСТЭК России;

б) Договоренностью между субъектом КИИ и ФСТЭК России;

в) Субъектом КИИ;

г) Не определяются.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Объекты и субъекты КИИ. Права и обязанности субъектов КИИ.

2. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ.

3. Основные понятия, термины и определения в области обеспечения безопасности значимых объектов КИИ.

4. Система нормативных правовых актов по вопросам обеспечения безопасности КИИ Российской Федерации.

5. Система безопасности значимого объекта КИИ. Цели и задачи системы безопасности значимого объекта КИИ.

6. Права и обязанности субъектов критической информационной инфраструктуры.

7. Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления.

8. Методы определения и оценки возможностей (потенциала) внешних и внутренних нарушителей.

9. Оценка возможных последствий реализации угроз безопасности информации в значимом объекте КИИ.

10. Правила и порядок категорирования объектов КИИ.

11. Реестр значимых объектов КИИ. Цель ведения реестра. Сведения, вносимые в реестр значимых объектов КИИ.

12. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значения.

13. Выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности.

14. Формирование перечня объектов КИИ Российской Федерации, подлежащих категорированию.

15. Определение вида и типа программных и программно-аппаратных средств защиты информации, обеспечивающих реализацию технических мер по обеспечению безопасности значимого объекта КИИ.

16. Реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта КИИ.

17. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов КИИ.

18. Требования к применяемым средствам защиты информации, к проведению их оценки на соответствие требованиям безопасности.

19. Требования к созданию систем безопасности значимых объектов КИИ Российской Федерации и обеспечению их функционирования.

20. Этапы жизненного цикла системы безопасности значимого объекта КИИ.

21. Стадии (этапы) работ по созданию систем безопасности значимого объекта КИИ.

22. Внедрение системы безопасности значимого объекта КИИ.

23. Контроль за обеспечением уровня безопасности значимого объекта КИИ.

24. Оценка соответствия значимых объектов КИИ требованиям по безопасности.

25. Документирование процедур и результатов контроля за обеспечением уровня безопасности значимого объекта КИИ.

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.Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа: пособие. – Воронеж: Кварта, 2015. – 440 с.

2.Воронов В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. – М.: Горячая линия – Телеком, 2013.

3.Программно-аппаратная защита информации: учебное пособие/ П.Б. Хорев. – М.: Форум, 2012. – 352 с.

4.Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ДМК Пресс, 2011. – 416 с.;

7.2 Дополнительная литература

1. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

4. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

5. Указ Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

6. Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утверждены постановлением Правительства Российской Федерации от 17 февраля 2018 г. № 162.

7. Правила категорирования объектов критической информационной инфраструктуры Российской Федерации. Утверждены постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

8. Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значения. Утвержден постановлением Правительства Российской Федерации от 8 февраля 2018 г

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

1. Банк данных угроз безопасности информации www.bdu.fstec.ru;
2. Информационно-справочные и поисковые системы: www.pravo.gov.ru, www.fstec.ru, www.gost.ru/wps/portal/tk362/;
3. Правовые справочные-поисковые системы («Гарант», «Консультант Плюс»);
4. http://elibrary.ru/. Научная электронная библиотека;
5. http://dspace.kgsu.ru/xmlui/ Электронная библиотека КГУ.

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Информационно-справочная система «КонсультантПлюс».

Для проведения лекций необходим специализированный учебный класс с минимальным оборудованием и программным обеспечением: Автоматизированное рабочее место преподавателя в составе: ПЭВМ. Проектор LCD (технологии DLP). Экран (интерактивный). Операционная система (Windows xp). Офисные программы (library office, MS Office). Антивирусные программы (MS Essential).

Для проведения практических занятий необходим специализированный компьютерный класс с минимальным оборудованием и программным обеспечением:

Автоматизированное рабочее место преподавателя в составе: ПЭВМ. Проектор LCD(технологии DLP). Экран (обычный). Операционная система(Windows xp). Офисные программы (library office, MS Office). Антивирусные программы (MS Essential). Автоматизированное рабочее место обучающегося (в расчете – одно рабочее место на одного обучающегося) в составе: ПЭВМ. Операционная система (Windows xp, 8, 10). Офисные программы (library office, MS Office). Антивирусные программы (MS Essential, MS defender). Программное обеспечение для проведения компьютерных тестов (KASS, Modul, Teams).

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet, коммутатор 2-го уровня D-LINK DGS-101D/E1A.

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

«Обеспечение безопасности значимых объектов критической информационной инфраструктуры»

образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Специализация: (специализация №5)

Безопасность открытых информационных систем

Трудоемкость дисциплины: 3 з.е. (108 академических часа)
*Семестр:*11 (очная форма обучения)
Форма промежуточной аттестации: экзамен

Содержание дисциплины. Основные разделы

Правовые основы обеспечения безопасности КИИ Российской Федерации. Угрозы безопасности информации, обрабатываемой на объектах КИИ. Категорирование объектов КИИ. Требования по обеспечению безопасности значимых объектов КИИ. Система безопасности объекта КИИ.