

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

СОГЛАСОВАНО

Декан ФИТ
Авдеев

А.С.

Рабочая программа дисциплины

Код и наименование дисциплины: Б1.В.ДВ.2.1 «Особенности защиты информации объектов критической информационной инфраструктуры»

**Код и наименование направления подготовки (специальности): 10.03.01
Информационная безопасность**

Направленность (профиль, специализация): Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)

Статус дисциплины: элективные дисциплины (модули)

Форма обучения: очная

Статус	Должность	И.О. Фамилия
Разработал	доцент	Е.В. Шарлаев
Согласовал	Зав. кафедрой «ИВТиИБ»	А.Г. Якунин
	руководитель направленности (профиля) программы	Е.В. Шарлаев

г. Барнаул

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

Компетенция	Содержание компетенции	Индикатор	Содержание индикатора
ПК-4	Способен участвовать в исследованиях защищенности объектов и средств защиты	ПК-4.1	Демонстрирует знание методов исследования защищенности объектов и средств защиты
		ПК-4.2	Предлагает методы исследования объектов информатизации с учетом их особенностей

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Информационные процессы и системы, Методы и средства криптографической защиты информации, Организационное и правовое обеспечение информационной безопасности, Программно-аппаратные средства защиты информации, Сети и системы передачи информации, Технологии защиты информации в вычислительных сетях
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Комплексная защита объектов информатизации, Подготовка к процедуре защиты и защита выпускной квалификационной работы, Преддипломная практика, Разработка организационно-распорядительной документации по защите информации

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 5 / 180

Форма промежуточной аттестации: Экзамен

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	32	48	0	100	90

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Форма обучения: очная

Семестр: 7

Лекционные занятия (32ч.)

- 1. Введение {дискуссия} (4ч.)[4,5,9,10] Субъекты и объекты КИИ: понятия, определения, принадлежности**
- 2. Законодательство Российской Федерации в области защиты критической информационной инфраструктуры {беседа} (4ч.)[4,5,9,10] Анализ Отечественной нормативно-методической базы по вопросам обеспечения безопасности объектов КИИ**
- 3. Объекты КИИ {дискуссия} (4ч.)[4,5,9,10] Объекты КИИ: классификация, многообразие, типы и виды. Определение бизнес-процессов. Составление Реестра бизнес-процессов. Оценка критичности бизнес-процессов. Определение и формирование Перечня объектов КИИ**
- 4. Категорирование объектов КИИ {беседа} (4ч.)[4,5,8,9,10] Категорирование объектов КИИ: многообразие, принципы, процедура и этапы. Описание процесса «Категорирование объектов КИИ». Расчет показателей критериев значимости объектов КИИ**
- 5. Обеспечение безопасности значимых объектов КИИ {беседа} (4ч.)[4,5,8,9,10] Создание системы безопасности значимых объектов КИИ. Рекомендации по обеспечению безопасности значимых объектов КИИ после завершения категорирования**
- 6. Взаимодействие с ГосСОПКА {беседа} (4ч.)[4,5,9,10] Выбор Центра ГосСОПКА. Организация сбора и обмена информацией о компьютерных инцидентах**
- 7. Совмещение объектов защиты. {лекция с разбором конкретных ситуаций} (4ч.)[4,5,7,8,9,10] Обзор типовых объектов защиты информатизации как объектов КИИ**
- 8. Аутсорсинг услуг. {беседа} (4ч.)[4,5,6,8,9,10] Привлечение лицензированных компаний с сертифицированными специалистами для защиты объектов КИИ.**

Лабораторные работы (48ч.)

- 1. Определение и формирование Перечня объектов КИИ. {работа в малых группах} (8ч.)[2,3,9,10,11,12,13,14] Определение и нормативное закрепление состава защищаемых объектов КИИ организации. Сбор и анализ нормативно-методической базы объектов КИИ организации.**
- 2. Ревизия систем, имеющих в организации. Оценка задействованности ИС, ИТКС, АСУ в бизнес-процессах. {работа в малых группах} (4ч.)[2,3,8,9,10,11,12,13,14] Составление Реестра бизнес-процессов. Оценка критичности бизнес-процессов. Формирование Перечня потенциально значимых объектов КИИ.**
- 3. Категорирование объектов КИИ {работа в малых группах} (8ч.)[2,3,8,9,10,11,12,13,14] Состав процессов, осуществляемых при категорировании объектов КИИ организации. Содержание этапов процесса определения бизнес-процессов организации. Содержание этапов процесса определения и формирования Перечня объектов КИИ**

организации. Формирование Реестра бизнес-процессов организации. Оформление сведений о результат категорирования.

4. Определение сценария реализации компьютерных атак на объекты КИИ. {работа в малых группах} (4ч.) [3,8,9,10,11,12,13,14] Формирование состава возможных событий (инцидентов), которые могут возникнуть в результате реализации наихудшего сценария целенаправленных компьютерных атак на ИС, ИТКС, АСУ.

5. Расчет показателей критериев значимости объектов КИИ. {работа в малых группах} (8ч.) [8,9,10,11,12,13,14] Порядок подготовки заключения о присвоении объекту КИИ организации одной из категорий значимости. Оформление Акта категорирования объекта КИИ. Пересмотр категории значимости объектов КИИ.

6. Обеспечение безопасности значимых объектов КИИ после завершения категорирования. {работа в малых группах} (8ч.) [8,9,10,11,12,13,14] Создание системы безопасности значимых объектов КИИ. Организация взаимодействия с центрами ГосСОПКА.

7. Исследование системы безопасности объектов КИИ организации на отказоустойчивость с учётом их особенностей и реагирование на компьютерные инциденты. {работа в малых группах} (8ч.) [3,4,6,8,9,10,11,12,13,14] Составление сценария проведения компьютерных атак на объекты КИИ. Реализация сценария компьютерных атак. Реагирование и оценка реагирование системы безопасности субъекта КИИ на сценарий проведения компьютерных атаки. Оформление результатов киберучения на реагирование системы безопасности субъекта КИИ на сценарий проведения компьютерных атаки.

Самостоятельная работа (100ч.)

1. Подготовка к текущим занятиям {с элементами электронного обучения и дистанционных образовательных технологий} (64ч.) [1,2,3,4,5,6,7,8,9,10,11,12,13,14]

2. Подготовка к экзамену {с элементами электронного обучения и дистанционных образовательных технологий} (36ч.) [2,3,4,5,6,7,8,9,10,11,12,13,14]

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронной информационно-образовательной среде АлтГТУ:

1. Загинайлов Ю. Н. Правовое обеспечение компьютерной безопасности: учебно-методическое пособие.-2-е изд., испр. и доп. / Ю. Н. Загинайлов; Алт. гос. техн. ун-т им. И.И. Ползунова.- Баранаул: Изд-во

АлтГТУ.- 2018 – 116 с. Прямая ссылка:
<http://elib.altstu.ru/eum/download/ivtib/uploads/zaginyaylov-yu-n-ivtiib-5a6ae9603068e.pdf>

2. Загинайлов Ю. Н. Управление информационной безопасностью: курс визуальных лекций / Ю.Н. Загинайлов; Алт.гос.техн.ун-т им.И.И.Ползунова.- Барнаул: Изд-во АлтГТУ.-2016- 125 с. Прямая ссылка: <http://elib.altstu.ru/eum/download/ivtib/uploads/zaginyaylov-yu-n-ivtiib-586224a37ee70.pdf>

3. Кошелев А.А., Шарлаев Е.В. Игровой тренинг - имитации, поиск, эксплуатации и устранения уязвимостей. Лабораторный практикум: учебнометодическое пособие; Алт. гос. техн. ун – т им. И.И. Ползунова, - Барнаул: 2017. - 71 с. Прямая ссылка: http://elib.altstu.ru/eum/download/ivtib/KoshelevSharlaev_IgrTrenIEUU_ump.pdf

6. Перечень учебной литературы

6.1. Основная литература

4. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – 2-е изд. – Саратов : Профобразование, 2019. – 702 с. – ISBN 978-5-4488-0070-2. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: <https://www.iprbookshop.ru/87995.html> (дата обращения: 06.03.2023).

5. Брюхомицкий, Ю. А. Безопасность информационных технологий : учебное пособие: в 2 частях: [16+] / Ю. А. Брюхомицкий; Южный федеральный университет. – Ростов-на-Дону ; Таганрог: Южный федеральный университет, 2020. – Ч. 1. – 171 с.: ил., табл., схем., граф. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=612167> (дата обращения: 24.06.2021). – Библиогр. в кн. – ISBN 978-5-9275-3571-2 (Ч. 1). – ISBN 978-5-9275-3526-2. – Текст: электронный.

6.2. Дополнительная литература

6. Белоус, А. И. Основы кибербезопасности: стандарты, концепции, методы и средства обеспечения : [16+] / А. И. Белоус, В. А. Солодуха. – Москва : Техносфера, 2021. – 482 с. : схем., ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=617523> (дата обращения: 06.03.2023). – ISBN 978-5-94836-612-8. – Текст : электронный.

7. Семенов, Ю. А. Алгоритмы телекоммуникационных сетей. Часть 1. Алгоритмы и протоколы каналов и сетей передачи данных : учебное пособие / Ю. А. Семенов. – 4-е изд. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. – 757 с. – ISBN 978-5-4497-1634-7. – Текст : электронный // Цифровой

образовательный ресурс IPR SMART : [сайт]. – URL: <https://www.iprbookshop.ru/120470.html> (дата обращения: 06.03.2023).

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

8. Документы по обеспечению безопасности критической информационной инфраструктуры <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoy-informatsionnoj-infrastruktury/290-inye#>

9. Безопасность объектов критической информационной инфраструктуры организации http://aciso.ru/files/docs/metodichka_2.0.pdf

10. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения <https://minzdrav.gov.ru/documents/9646-metodicheskie-rekomendatsii-po-kategorirovaniyu-ob-ektov-kriticheskoy-informatsionnoy-infrastruktury-sfery-zdravoohraneniya>

11. Официальный сайт Совета Безопасности Российской Федерации <http://www.scrf.gov.ru/>

12. Официальный сайт Федеральной службы по техническому и экспортному контролю <https://fstec.ru/>

13. Официальный сайт Федеральной службы безопасности Российской Федерации <http://www.fsb.ru/>

14. Интернет-издание о высоких технологиях <https://www.cnews.ru/>

8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

№пп	Используемое программное обеспечение
1	LibreOffice
1	Foxit Reader

№пп	Используемое программное обеспечение
2	Windows
2	GIMP
3	Антивирус Kaspersky
6	Гарант
7	7-Zip

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	Национальная электронная библиотека (НЭБ) – свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. (http://нэб.рф/)

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Наименование специальных помещений и помещений для самостоятельной работы
учебные аудитории для проведения учебных занятий
помещения для самостоятельной работы

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».