

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета

Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины
Обеспечение безопасности критической информационной инфраструктуры

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 26.04.2024, протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 03.05.2024

1. Цели освоения дисциплины

Дисциплина «Обеспечение безопасности критической информационной инфраструктуры» призвана обеспечить освоение студентами теоретических и практических навыков работы с нормативными правовыми актами в области обеспечения информационной безопасности объектов критической информационной инфраструктуры (далее – объекты КИИ), в том числе нормативными методическими документами ФСБ России и ФСТЭК России, и применения их положений в профессиональной деятельности.

Данная дисциплина раскрывает основы правового регулирования отношений в сфере безопасности объектов КИИ, понятия и виды субъектов и объектов КИИ по законодательству Российской Федерации, а также нормативные требования ФСБ и ФСТЭК России к субъектам КИИ.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Обеспечение безопасности критической информационной инфраструктуры» относится к вариативной части образовательной программы и является факультативной дисциплиной.

Для успешного усвоения данной дисциплины необходимо, чтобы студент овладел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин «Основы управленческой деятельности», «Организационное и правовое обеспечение информационной безопасности».

Знания и навыки, полученные в результате изучения дисциплины «Обеспечение безопасности критической информационной инфраструктуры», используются студентами в дальнейшем при разработке курсовых и дипломных работ.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
Профессиональные компетенции	
ПК-16 Обладает способностью разрабатывать проекты нормативных правовых актов и методические материалы, регламентирующие работу по обеспечению информационной безопасности компьютерных систем	Знать: - основные нормативные правовые акты в области обеспечения информационной безопасности КИИ и нормативные методические документы ФСБ России и ФСТЭК России в области защиты КИИ. Уметь: - применять основные нормативные правовые акты в области обеспечения безопасности КИИ и нормативные методические документы ФСБ России и ФСТЭК России в области защиты КИИ. - планировать мероприятия по категорированию и обеспечению безопасности КИИ; - выявлять процессы, связанные с категорированием КИИ; - разрабатывать необходимые документы и локальные нормативные акты по обеспечению безопасности КИИ; - определять класс информационных систем и уровень защищенности

	информации; - обеспечивать безопасность КИИ; - организовывать обмен информацией об инцидентах с НКЦКИ России.
--	---

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 акад. часа.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Актуальность и проблематика защиты критической информационной инфраструктуры	А	1					2	Устный опрос.
2	Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры	А	2					4	Устный опрос.
3	Определение субъекта КИИ	А	1	2		1		4	Устный опрос.
4	Выделение критических для деятельности процессов	А	2					4	Устный опрос.
5	Правила категорирования объектов КИИ	А	1	3				4	Устный опрос.
6	Взаимодействие с ФСБ России по безопасности КИИ	А	1	2		1		3	Устный опрос.
7	Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры	А	3	4		1		4	Устный опрос.
8	Организация внутреннего контроля значимых объектов КИИ	А	1					4	Устный опрос.
9	Обеспечение бесперебойной эксплуатации значимых объектов КИИ	А	3	4		1		6	Устный опрос.

							0,3	2,7	Зачет
	Всего		15	15		4	0,3	37,7	

Содержание разделов дисциплины:

Тема 1. Актуальность и проблематика защиты критической информационной инфраструктуры.

1.1. Введение в тематику защиты значимых объектов критической информационной инфраструктуры.

1.2. Информационная инфраструктура России. Понятие критической информационной инфраструктуры (КИИ).

1.3. Обеспечение безопасности критической информационной инфраструктуры в иностранных государствах.

Тема 2. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры.

2.1. Основные термины. Уполномоченные органы (регуляторы) в сфере обеспечения безопасности КИИ. Права и обязанности субъектов КИИ.

2.2. Алгоритм мероприятий по реализации требований ФЗ № 187-ФЗ. Анализ нормативно-правовых актов в сфере КИИ.

2.3. Уголовная и административная ответственность субъектов КИИ.

Тема 3. Определение субъекта КИИ.

3.1. Получение информации о видах деятельности организаций.

3.2. Определение относимости организации к субъектам КИИ.

Тема 4. Выделение критических для деятельности процессов.

4.1. Процессный подход

4.2. Сбор информации о процессах

4.3. Анализ бизнес-процессов

4.4. Выделение критических процессов,

Тема 5. Правила категорирования объектов КИИ.

5.1. Разбор положений Постановления Правительства РФ № 127 «Об утверждении Правил категорирования объектов КИИ, а также показателей критериев значимости объектов КИИ РФ и их значений»

5.2. Выделение и учет объектов КИИ. Определение критериев значимости объектов КИИ РФ и их значений. Определение категории значимости объектов КИИ и подготовка сведений о категорировании для направления во ФСТЭК России.

5.3. Положения приказа ФСТЭК России № 236 "Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий"

Тема 6. Взаимодействие с ФСБ России по безопасности КИИ.

6.1. Характеристика приказов ФСБ России в сфере КИИ.

6.2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) в соответствии с приказом ФСБ России № 367 "Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА"

6.3. Приказ ФСБ России № 366 "О Национальном координационном центре по компьютерным инцидентам". Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ в соответствии с приказом ФСБ России № 368.

6.4. Разработка регламента управления инцидентами и плана реагирования на компьютерные инциденты.

Тема 7. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры

7.1. Анализ требований к обеспечению безопасности значимых объектов КИИ в соответствии с ФЗ № 187, приказом ФСТЭК № 239 "Об утверждении Требований по обеспечению безопасности ЗО КИИ РФ", приказом ФСТЭК № 235 "Об утверждении Требований к созданию систем безопасности ЗО КИИ РФ и обеспечению их функционирования"

7.2. Разработка организационных и технических мер по обеспечению безопасности значимого объекта КИИ. Разработка рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности). Порядок аттестации значимых объектов КИИ.

Тема 8. Организация внутреннего контроля значимых объектов КИИ

8.1. Регламент аудита информационной безопасности.

8.2. Аудит информационной безопасности. План мероприятий по реагированию на компьютерные инциденты и мерами по ликвидации последствий компьютерных атак.

Тема 9. Обеспечение бесперебойной эксплуатации значимых объектов КИИ

9.1. Обеспечение безопасности значимых объектов КИИ в ходе их эксплуатации. Обеспечение безопасности значимых объектов КИИ при выводе их из эксплуатации.

9.2. Подключение значимых объектов КИИ к госСОПКА.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний по предложенному алгоритму.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации:

- программы Microsoft Office;
- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php
- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента»
<https://www.studentlibrary.ru>
- Некоммерческая (бесплатная) Интернет-версия справочной системы Гарант.
<http://ivo.garant.ru/#/startpage:0>
- Официальный интернет-портал правовой информации
<http://publication.pravo.gov.ru>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

а) основная литература

1. ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности»
<http://gost.gtsever.ru/Data/578/57828.pdf?ysclid=lj7kswcvmq104399254>
2. Демидов О. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества - Москва: Альпина Паблишер, 2016.
<https://www.studentlibrary.ru/ru/doc/ISBN9785998808456-SCN0000/000.html>
3. Гродзенский, Я. С. Информационная безопасность : учебное пособие / Гродзенский Я. С. - Москва : РГ-Пресс, 2020. - 144 с. - ISBN 978-5-9988-0845-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785998808456.html>

б) дополнительная литература:

1. «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», утверждена Президентом РФ 12.12.2014 № К 1274.
<http://www.fsb.ru/fsb/npd/more.htm%21id%3D10437638%40fsbNpa.html>
2. Информационное сообщение ФСТЭК России №240/25/3752 от 24.08.2018 «По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».
<https://www.garant.ru/products/ipo/prime/doc/71935164/?ysclid=lj7172ljt5249847942>
3. Методические рекомендации по проведению категорирования объектов критической информационной инфраструктуры, «СТЭП ЛОДЖИК», 2020.
<https://check-ib.ru/wp-content/uploads/Metodicheskie-rekomendatsii-po-kategorirovaniyu.StepLogic.pdf?ysclid=lj712imnhh49554122>
4. Методические рекомендации по определению объектов критической информационной инфраструктуры и категорий значимости объектов критической

информационной инфраструктуры, ДИТ города Москвы, 2020 год, электронное издание: https://wikisec.ru/images/9/94/Метреки_по_КИИ_ДИТ_Москвы.pdf

5. Farrand B. Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism / B. Farrand, H. Carrapico // Security Privatization: How Non-Security-Related Private Businesses Shape Security Governance. – Basel: Springer International Publishing AG, 2018. P. 197 – 217.

6. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. Official Journal L, 345(23), 12. <https://eur-lex.europa.eu/eli/dir/2008/114/oj>

7. Green Paper on a European Programme for Critical Infrastructure Protection. COM 576 final (2005).

<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52005DC0576>

в) законодательные документы

1. Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации».

<http://publication.pravo.gov.ru/Document/View/0001201707260023?ysclid=lj7kozqddt646039800>

2. Указ Президента РФ № 31с от 15.01.2013 «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

<http://publication.pravo.gov.ru/Document/View/0001201301210012?ysclid=lj7kocnaxu862513041>

3. Указ Президента РФ № 646 от 05.12.2016 «Об утверждении Доктрины информационной безопасности Российской Федерации».

<http://publication.pravo.gov.ru/Document/View/0001201612060002?ysclid=lj7knwsvcj687403019>

4. Постановление Правительства РФ № 127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры РФ и их значений».

<http://publication.pravo.gov.ru/Document/View/0001201802130006?ysclid=lj7kndtg1m834325974>

5. Постановление Правительства РФ № 162 от 17.02.2018 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры РФ».

<http://publication.pravo.gov.ru/Document/View/0001201802210006?ysclid=lj7kmufq8a626793560>

6. Приказ ФСТЭК России № 227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры РФ».

<https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-6-dekabrya-2017-g-n-227?ysclid=lj7kmct1qm645110525>

7. Приказ ФСТЭК России № 229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности ЗО КИИ РФ».

<https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-dekabrya-2017-g-n-229?ysclid=lj7klkqdoj538476649>

8. Приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности ЗО КИИ РФ и обеспечению их функционирования». <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235?ysclid=lj7kl0hzhv947120001>

9. Приказ ФСТЭК России № 236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий». <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236?ysclid=lj7kjm2cy98389939>
10. Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности ЗО КИИ РФ». <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239?ysclid=lj7kjl1c1g884854034>
11. Приказ ФСБ России № 366 от 24.07.2018 «О Национальном координационном центре по компьютерным инцидентам». <http://publication.pravo.gov.ru/Document/View/0001201809100001?ysclid=lj7kiye4bo122327606>
12. Приказ ФСБ России № 367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА». <http://publication.pravo.gov.ru/Document/View/0001201809100002?ysclid=lj7kijxosx452263206>
13. Приказ ФСБ России № 368 от 24.07.2018 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации». <http://publication.pravo.gov.ru/Document/View/0001201809100003?ysclid=lj7khwtm615174214>
14. Приказ ФСБ России № 281 от 19.06.2019 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации». <http://publication.pravo.gov.ru/Document/View/0001201907170027?ysclid=lj7kh8rtgc51223905>
15. Приказ ФСБ России № 196 от 06.05.2019 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты». <http://publication.pravo.gov.ru/Document/View/0001201905310017?ysclid=lj7kgh6a5h498888711>

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине.

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;

- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор:

старший преподаватель кафедры КБ и ММОИ А.В.

Саханда А.В.

**Приложение №1 к рабочей программе дисциплины
«Обеспечение безопасности критической информационной инфраструктуры»**

**Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине**

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,

Список вопросов для опроса на практических занятиях

1. Каковы составляющие российской системы обеспечения безопасности критических информационных систем от компьютерных атак?
2. Каковы функции участников реализации системы обеспечения безопасности критических информационных систем от компьютерных атак?
3. Как определить критические процессы на предприятии (в организации).
4. Критерии отнесения информационных систем к объектам КИИ.
5. Требования приказов ФСТЭК в отношении КИИ.
6. Требования приказов ФСБ в отношении КИИ.
7. Взаимодействие с госСОПКА.
8. Подготовка организационно-распорядительной документации по категорированию значимых объектов КИИ.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету

1. Информация, характеристики безопасности информации.
2. Информация как объект правовых отношений.
3. Обладатель информации и оператор информационной системы: их права и обязанности.
4. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации, положения кодекса об административных правонарушениях и уголовного кодекса.
5. Информационная инфраструктура России.
6. Понятие критической информационной инфраструктуры (КИИ).
7. В какие сферы деятельности входят значимые объекты КИИ?
8. Задачи ФСТЭК России в сфере безопасности информации и объектов КИИ.
9. Задачи ФСБ России в сфере безопасности информации и объектов КИИ.
10. Какие основные НПА в сфере безопасности значимых объектов КИИ
11. Определение относимости организации к субъекту КИИ.
12. Выделение критических процессов.
13. Подготовка реестра КИИ для направления во ФСТЭК.
14. Расскажите алгоритм категорирования объектов КИИ.
15. Как определяются критерии значимости объектов КИИ РФ и их значения?
16. Какие сведения об объектах КИИ необходимо направлять во ФСТЭК России.
17. Какие сведения об объектах КИИ необходимо направлять в ФСБ России.
18. Что из себя представляет и зачем нужна госСОПКА?
19. Зачем необходимо направлять информацию в госСОПКУ?
20. Цели и задачи НКЦКИ.

21. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.
22. Организационные и технические меры по обеспечению безопасности значимого объекта КИИ.
23. Порядок аттестации значимых объектов КИИ.
24. Аудит информационной безопасности.
25. Мероприятия по реагированию на компьютерные инциденты и меры по ликвидации последствий компьютерных атак.
26. Обеспечение безопасности значимых объектов КИИ в ходе их эксплуатации.
27. Обеспечение безопасности значимых объектов КИИ при выводе их из эксплуатации.
28. Подключение объектов КИИ к госСОПКА.

3. Правила приема зачета.

Оценка знаний по итогу прохождения курса проводится в форме принятия зачета.

На зачете проверяется сформированность всех указанных в учебной программе компетенций.

В билет для зачета включаются два теоретических вопроса. На подготовку к ответу дается не менее 1 академического часа.

По итогам ответов студенту выставляется одна из оценок: «зачтено», «не зачтено».

Оценка «зачтено» выставляется студенту, если: он знает основные определения, последователен в изложении материала, демонстрирует базовые знания дисциплины, владеет необходимыми умениями и навыками при выполнении практических заданий.

Оценка «не зачтено» выставляется студенту, если: он не знает основных определений, непоследователен и сбивчив в изложении материала, не обладает определенной системой знаний по дисциплине, не в полной мере владеет необходимыми умениями и навыками при выполнении практических заданий.

Оценка «не зачтено» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

Приложение №2 к рабочей программе дисциплины «Обеспечение безопасности критической информационной инфраструктуры»

Методические указания для студентов по освоению дисциплины

Изучение дисциплины предполагает уверенное владение компьютером, умение осуществлять поиск и оценку достоверности необходимой информации в сети Интернет, но студенту достаточно сложно самостоятельно освоить вопросы дисциплины «Обеспечение безопасности критической информационной инфраструктуры». Посещение всех предусмотренных аудиторных занятий является совершенно необходимым в силу обучения на них учащихся сравнительным оценкам знаний из различных источников, критической их оценки. Также без упорных и регулярных самостоятельных занятий в течение семестра, желательно с «упреждающим знакомством» с содержанием предстоящего занятия, крайне сложно усвоить логику и аргументацию упомянутых сравнительных оценок и критического анализа знаний из различных источников, что не позволит студентам развить продвинутого и высокого уровня компетенций.