МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
«28 » мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Безопасность критической информационной инфраструктуры»

Направление подготовки
10.03.01 «Информационная безопасность»

Образовательная программа (профиль)
«Безопасность компьютерных систем»

Квалификация (степень) выпускника
Бакалавр

Форма обучения
Очная

Год приема – 2020

Москва -2020

1. Цели освоения дисциплины

Основными целями освоения дисциплины «Безопасность критической информационной инфраструктуры» являются:

- теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по защите объектов информатизации критически важных объектов.

К **основным задачам** освоения дисциплины «Безопасность критической информационной инфраструктуры» «следует отнести:

- изучение системы государственного контроля в области обеспечения информационной безопасности на критически важных объектах и системы признаков критически важных объектов;
- обучение принципам анализа с целью выявления потенциальных уязвимостей информационной безопасности на критически важных объектах;
- выработка умений классифицировать и оценивать угрозы информационной безопасности для критически важных объектов, эффективно использовать различные методы и средства защиты информации;
- изучение основных средств и способов обеспечения информационной безопасности на критически важных объектах, принципов построения систем защиты информации.

2. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Безопасность критической информационной инфраструктуры» относится к числу профессиональных учебных дисциплин специализации базовой части цикла (Б.1.1.42) основной образовательной программы бакалавриата

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Безопасность жизнедеятельности», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации», «Управление информационной безопасностью», «Программно-аппаратные средства обеспечения информационной безопасности».

3. Перечень планируемых результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины «Безопасность критической информационной инфраструктуры» у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать	Перечень планируемых результатов обучения по дисциплине
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**знать:** -нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности критически важных объектов; **уметь:** - реализовывать с учетом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации по вопросам защиты информации ограниченного доступа;

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет **3** зачетных единицы, т.е.108 академических часа (лабораторные занятия – 54 часа, самостоятельная работа - 54 часа), форма контроля – **экзамен** в **7** семестре.

Структура и содержание дисциплины «Обеспечение информационной безопасности на критически важных объектах» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема 1. Общая характеристика критически важных объектов РФ

Понятие объекта, критически важного для национальной безопасности государства. Приоритетные направления обеспечения национальной безопасности РФ. Критические факторы национальной безопасности. «Концепция национальной безопасности РФ». Понятия критически важной инфраструктуры, критически важного объекта и информационного критически важного объекта (системы управления критически важным объектом).

Классификация критически важных объектов. Объекты федерального уровня, уровня субъекта Российской Федерации, территориального и муниципального уровней. Объекты ядерно-опасные, радиационно-опасные, химически опасные, биологически опасные, техногенно-опасные, гидродинамически опасные, объекты информационной и телекоммуникационной инфраструктуры РФ.

Классификация критически важных объектов по уровням угроз. Государственный стандарт Российской Федерации ГОСТ Р 22.0.02-94 «Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий». Угрозы информационной безопасности «верхнего уровня».

Тема 2. Признаки принадлежности к критически важным объектам

Признаки критически важных объектов. Систематизация и общие характеристики объектов, значимых с позиции национальной безопасности. «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-

телекоммуникационных систем к числу, защищаемых от деструктивных информационных воздействий», утвержденная Секретарем Совета безопасности РФ 8 ноября 2005 г.

Тема 3. Последствия нарушения функционирования критически важных объектов

Нарушения функционирования критически важных объектов. Нарушение системы обеспечения жизнедеятельности городов и населенных пунктов. Гибель или травмирование людей. Нарушение социальной стабильности в стране, регионе, субъектах федерации. Аварии, катастрофы, разрушение или заражение среды обитания в национальном масштабе. Нанесение крупного экономического ущерба государству. Крупномасштабное уничтожение национальных ресурсов.

Тема 4. Информационная безопасность объектов критически важных инфраструктур

Информационная безопасность как важная составляющая национальной безопасности. Особенности обеспечения информационной безопасности для объектов важных с позиции национальной безопасности. «Доктрина информационной безопасности РФ». Основные принципы обеспечения информационной безопасности таких объектов. Программно-технический и операционный уровни обеспечения безопасности.

Тема 5. Контроль мер обеспечения информационной безопасности на критически важных объектах.

Государственные органы РФ, контролирующие деятельность в области защиты информации. ФСТЭК России. Функции ФСБ России по разработке и утверждению нормативных и методических документов по вопросам обеспечения информационной безопасности информационно-телекоммуникационных систем и сетей критически важных объектов, по контролю обеспечения информационной безопасности указанных систем и сетей.

Службы обеспечения информационной безопасности в составе федеральных органов государственной власти.

Службы, организующие защиту информации на уровне предприятия. Служба экономической безопасности. Служба безопасности персонала (Режимный отдел). Отдел кадров. Служба информационной безопасности.

Тема 6. Нормативная база, регламентирующая обеспечение информационной безопасности критически важных объектов.

Методические документы государственных органов России. Руководящие документы ФСТЭК (Гостехкомиссии России). Приказы ФСБ.

Методические документы ФСТЭК, необходимые для разработки модели угроз. Систематизация сведений о возможных угрозах безопасности информации на типовых объектах информатизации. «Базовая модель угроз безопасности информации в ключевых системах

информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007). «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007).

Требования по организации обеспечения безопасности информации в ключевых системах информационной инфраструктуры. Признаки и критерии отнесения систем информационной инфраструктуры к ключевым системам. «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007). «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007)

Тема 7. Особенности обеспечения информационной безопасности критически важных объектов

Определение угроз и уровней информационной безопасности критически важных объектов. Категорирование критически важных объектов в зависимости от негативных последствий, возникающих вследствие прекращения или нарушения их функционирования.

Уязвимости критически важных объектов. Причины возникновения уязвимостей. Вывод из строя основных сервисов систем управления критически важных объектов. Отсутствие изолированности от внешней информационной среды. Несвоевременное обновление программных и аппаратных платформ. Использование незащищенных каналов связи. Человеческий фактор. Факторы окружающей среды. Оценка уязвимости объектов информационной и телекоммуникационной инфраструктуры и объектов информатизации от актов незаконного вмешательства и деструктивных информационных воздействий.

Оценка уязвимости критически важных объектов. Степень защищенности критически важных объектов от деструктивного информационного воздействия и актов незаконного вмешательства.

Тема 8. Требования по обеспечению безопасности критических информационных структур

Разработка требований по обеспечению информационной безопасности критически важных объектов. Концепция безопасности объекта. Организационные вопросы безопасности. Требования к оформлению концепции обеспечения информационной безопасности объекта. Вопросы безопасности, связанные с персоналом. Требования к классификации и управлению активами, связанными с информационно-телекоммуникационными системами.

Вопросы физической защиты и защиты от воздействий окружающей среды. Управление передачей данных и производственной деятельностью. Вопросы защиты от вредоносного программного обеспечения. Контроль доступа к информации и производственным процессам. Порядок разработки и обслуживания систем. Управление непрерывностью производственного процесса. Вопросы безопасности, связанные с радиоэлектронной защитой.

Требования безопасности при взаимодействии с открытыми (публичными) информационными системами и сетями. Обеспечение безопасности информационных технологий в ходе эксплуатации информационно-телекоммуникационных систем. Контроль систем на соответствие требованиям.

Тема 9. Организационно-технические и режимные меры информационной безопасности на критически важных объектах

Политика информационной безопасности критически важных объектов. Актуальность политик безопасности. Основные причины создания политик безопасности. Российская специфика разработки политик безопасности.

Реализация политик безопасности. Задание общих правил безопасности. Архитектура системы защиты информации на критически важном объекте. Настройки основных компонентов системы защиты критически важного объекта. Совершенствование правил безопасности.

Выработка политики информационной безопасности предприятия, относящегося к категории критически важного объекта. Выработка процедур для предупреждения нарушений безопасности. Типы процедур безопасности. Реакция на нарушение безопасности. Выработка мер, предпринимаемых после нарушения.

Разработка технических регламентов для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов

Тема 10. Разработка и реализация планов реагирования и восстановления после инцидентов безопасности критически важного объекта

План реагирования на инциденты. Классификация инцидентов безопасности критически важного объекта. Определение процедур, характеризующих и классифицирующих события, связанные с инцидентами физической и информационной безопасности. Сообщения об инцидентах безопасности КВОИ.

Мероприятия по реагированию на инциденты безопасности критически важного объекта. Роли и обязанности группы реагирования на инциденты. Первоочередные действия, которые необходимо предпринять при обнаружении инцидента. Контрмеры, необходимые для смягчения последствий и восстановления функционирования критически важного объекта до безопасного эксплуатационного состояния.

Разработка и реализация планов восстановления после инцидентов. План восстановления нормального функционирования КВОИ. Ресурсы, необходимые для успешной его реализации. Учет установленных требований к непрерывности операций и процессов объекта и методам и мерам восстановления после инцидентов. Процедуры реагирования и восстановления. Определение конкретных способов реагирования на инциденты различной длительности и тяжести. Поддержание в актуальном состоянии планов восстановления. Разработка плана тренировок, программы тренировок и повышения квалификации персонала, работа которого непосредственно связана с обеспечением безопасности критически важных объектов.

Тема 11. Построение системы защиты информации на критически важном объекте

Система защиты информации. Принципы, структурный состав и особенности построения системы защиты информации критически важного объекта.

Этапы создания систем защиты информации. Определение информационных и технических ресурсов, подлежащих защите. Выявление полного множества потенциально возможных угроз и

каналов утечки информации. Проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки. Определение требований к системе защиты. Осуществление выбора средств защиты информации и их характеристик. Внедрение и организация использования выбранных мер, способов и средств защиты. Осуществление контроля целостности и управление системой защиты.

Содержание работ по обеспечению безопасности информации на критически важном объекте. Определение уровня важности объекта. Выявление критически важной информации, циркулирующей на объекте. Выявление актуальных угроз безопасности информации. Распределение задач информационной безопасности на критически важном объекте. Решение финансовых, кадровых и материальных вопросов. Разработка технического задания на внедрение мер информационной безопасности на критически важном объекте и реализация этих мер. Оформление технического паспорта на систему обеспечения безопасности информации, проведение испытаний системы. Оформление организационных документов по информационной безопасности на критически важном объекте.

Тема 12. Средства защиты информации, использующиеся на критически важных объектах и оценка их эффективности

Выбор средств защиты информации. Анализ отечественного рынка средств защиты информации. Подходы к выбору средств защиты информации.

Программно-технические способы и средства обеспечения информационной безопасности. Сертифицированные отечественные средства предупреждения и обнаружения компьютерных атак и защиты информации, разрабатываемые и производимые лицензиатами федеральных органов исполнительной власти. Системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов. Восстановление работоспособности средств защиты информации, функционирующих на критически важных объектах.

Оценка эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов.

5. Образовательные технологии

Методика преподавания дисциплины «Безопасность критической информационной инфраструктуры» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- проведение лабораторных работ интерактивных занятий лекционного типа с использованием интерактивной доски;
- подготовка и проведение презентаций самостоятельных работ по темам дисциплины.

Удельный вес лабораторных работ по дисциплине составляет 70 % аудиторных занятий. Занятия лекционного типа, проводимые в интерактивных форме, составляют 30 % от объема аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение презентационных выступлений по выбранным направлениям технической защиты информации;
- экзамен в конце семестра.

Темы докладов и вопросы для экзамена приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

В результате освоения дисциплины формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК-4	способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты

В процессе освоения образовательной программы данная компетенция, в том числе ее отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин, практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины, описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине:

ПК-4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Показатель	**Критерии оценивания**

	2	3	4	5
знать: -нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности критически важных объектов;	Обучающийся демонстрирует полное отсутствие или недостаточное знание основных нормативно-методических и руководящих документов, регламентирующих обеспечение информационной безопасности критически важных объектов;	Обучающийся демонстрирует частичное (удовлетворительное) знание и понимание основных методических и руководящих документов, регламентирующих обеспечение информационной безопасности критически важных объектов;	Обучающийся демонстрирует полное знание и понимание основных методических и руководящих документов, регламентирующих обеспечение информационной безопасности критически важных объектов, но допускает незначительные ошибки.	Обучающийся демонстрирует полное знание и понимание основных методических и руководящих документов, регламентирующих обеспечение информационной безопасности критически важных объектов. Допускаются незначительные неточности
уметь: - реализовывать с учетом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации по вопросам защиты информации ограниченного доступа;	Обучающийся не умеет или в недостаточной степени умеет - реализовывать требования нормативно-методической и руководящей документации по вопросам защиты информации ограниченного доступа;	Обучающийся демонстрирует не в полной мере умение реализовывать требования нормативно-методической и руководящей документации по вопросам защиты информации ограниченного доступа	Обучающийся демонстрирует полное умение реализовывать требования нормативно-методической и руководящей документации по вопросам защиты информации, но допускает незначительные ошибки	Обучающийся демонстрирует полное умение реализовывать требования нормативно-методической и руководящей документации по вопросам защиты информации. Допускаются незначительные неточности

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	***Описание***
Отлично	*Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.*
Хорошо	*Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.*
Удовлетворительно	*Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.*
Неудовлетворительно	*Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.*

Фонд оценочных средств представлен в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература

Конспект лекций по дисциплине **«Безопасность критической информационной инфраструктуры»**

б) программное обеспечение и интернет-ресурсы:

1. Безопасность АСУ ТП критически важных объектов
http://www.secuteck.ru/articles2/security-director/bezopasnost-asu-tp-kriticheski-vazhnyh-obektov

2. Антитеррористическая защита критически важных объектов

http://www.arms-expo.ru›Новости›…-kriticheski-vazhnyh-ob…

3. Концепция противодействия терроризму в Российской Федерации

http://www.refdb.ru›look/2566466-pall.html

4. Комплексные решения противодействия терроризму на...
http://www.Secuteck.ru›…OPS…terrorizmu…kriticheski-vazhnyh…

Программное обеспечение: не предусмотрено

в) нормативно-правовые акты:

1. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации
2. Государственный стандарт Российской Федерации ГОСТ Р 22.0.02-94 «Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий».
3. Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий: утв. Секретарем Совета безопасности РФ 8 ноября 2005 г.
4. Решение Совета Безопасности РФ и президиума Госсовета РФ «О мерах по обеспечению защищенности критически важных для национальной безопасности объектов инфраструктуры и населения страны от угроз техногенного, природного характера и террористических проявлений» (протокол от 13.11.2003 г. № 4).
5. «Методические рекомендации по разработке Планов повышения защищенности критически важных объектов, территорий субъектов Российской Федерации и муниципальных образований» утвержденные заместителем министра МЧС России А.П. Чуприян 28.12.2011 года № 2-4-60-21-14.

8. Материально-техническое обеспечение дисциплины

Для проведения и лабораторных работ занятий лекционного типа необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран) – 1 комплект.

Компьютерный класс для самостоятельной работы, обеспечивающий доступ к сети Интернет, из расчета одно рабочее место на одного студента.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи с учебным планом. Основой теоретической подготовки студентов являются *лекции и нормативно-методические документы* по безопасности критических информационных инфраструктур.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Практические занятия предполагают проведение творческих дискуссий, активный обмен мнениями по рассматриваемым вопросам, заслушивание и обсуждение рефератов (докладов) по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении практического занятия преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, помогает с развертыванием и включением в работу программно-аппаратных комплексов, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на зачете.

Самостоятельная работа по дисциплине предполагает подготовку студентами презентаций (докладов) по заданным или выбранным темам. Самостоятельная работа студентов также предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины по доступным источникам. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:
- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:
- уровень освоения студентом учебного материала;
- умение студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01 «Информационная безопасность»**.

Программу составил: доцент, к.э.н. Рагозин Ю.Н.

Программа утверждена на заседании кафедры “Информационная безопасность”

«29» августа 2020 г., протокол № 1

Заведующий кафедрой

«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность автоматизированных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Безопасность критической информационной инфраструктуры»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Темы презентаций (докладов)
Экзамен

Составители: доцент к.э.н., Рагозин Ю.Н.

Москва, 2020 год

Таблица

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

«Безопасность критической информационной инфраструктуры»					
ФГОС ВО 10.03.01 «Информационная безопасность»					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **профессионально-специализированные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средств**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**знать:** -нормативно-методические и руководящие документы, регламентирующие обеспечение информационной безопасности критически важных объектов; **уметь:** - реализовывать с учетом особенностей функционирования критически важных объектов требования нормативно-методической и руководящей документации по вопросам защиты информации ограниченного доступа;	Лабораторные работы, занятия лекционного типа, самостоятельная работа	экзамен	**Базовый уровень:** способен участвовать в работах по реализации политики информационной безопасности критической информационной инфраструктуры

Оценочные средства для текущей аттестации

Примерные темы презентаций (докладов):

1. Классификация критически важных объектов информатизации по требованиям физической защиты с использованием методов кластерного анализа
2. Критерии защищенности ИТ- инфраструктур КВО
3. Состояние российской регулятивной базы для области ИБ КВО
4. Факторы, затрудняющие защиту ИТ-инфраструктур КВО
5. Состояние защищенности ИТ-инфраструктуры КВО в России
6. Информационная безопасность критически важных объектов
7. Требования безопасности к технологическим процессам
8. Назначение и состав АСУ ТП
9. Безопасность АСУ ТП критически важных объектов
10. . Политики информационной безопасности
11. Информационная безопасность: Нормативно-правовые аспекты
12. Критически важные объекты и кибертерроризм
13. Защита компьютерной информации. Эффективные методы и средства.
14. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты
15. Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий
16. Защита критически важных объектов России от угроз техногенного, природного характера и террористических актов.
17. Доктрина информационной безопасности Российской Федерации
18. Концепция национальной безопасности Российской Федерации
19. Государственный стандарт Российской Федерации ГОСТ Р 22.0.02-94 «Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий».
20. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации.
21. Системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов.
22. Оценка эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов.
23. Разработка технических регламентов для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов.

Оценочные средства для промежуточной аттестации

Экзамен

Список вопросов для экзамена по дисциплине

1. Понятие объекта, критически важного для национальной безопасности государства.
2.Понятия критически важной инфраструктуры, критически важного объекта и информационного критически важного объекта (системы управления критически важным объектом).
3. Классификация критически важных объектов по уровням угроз.
4. Последствия нарушения функционирования критически важных объектов.
5. Доктрина информационной безопасности РФ.
6. Государственные органы РФ, контролирующие деятельность в области защиты информации.
7. Службы, организующие защиту информации на уровне предприятия.
8. Требования по организации обеспечения безопасности информации в критических информационных инфраструктурах.
9. «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007).
10. Уязвимости критически важных объектов. Причины возникновения уязвимостей.
11. Оценка уязвимости критически важных объектов. Степень защищенности критически важных объектов от деструктивного информационного воздействия и актов незаконного вмешательства.
12. Концепция безопасности объекта. Организационные вопросы безопасности. Требования к оформлению концепции обеспечения информационной безопасности объекта.
13. Вопросы физической защиты и защиты от воздействий окружающей среды
14. Обеспечение безопасности информационных технологий в ходе эксплуатации информационно-телекоммуникационных систем.
15. Архитектура системы защиты информации на критически важном объекте.
16. Выработка политики информационной безопасности предприятия, относящегося к категории критически важного объекта.
17. Политика информационной безопасности. Актуальность политик безопасности. Основные причины создания политик безопасности. Российская специфика разработки политик безопасности.
18. Разработка технических регламентов для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов

19. Разработка и реализация планов восстановления после инцидентов.
20. Разработка плана тренировок, программы тренировок и повышения квалификации персонала, работа которого непосредственно связана с обеспечением безопасности критически важных объектов.
21. Принципы, структурный состав и особенности построения системы защиты информации критически важного объекта.
22. Этапы создания систем защиты информации
23. Содержание работ по обеспечению безопасности информации на критически важном объекте.
22. Оформление технического паспорта на систему обеспечения безопасности информации, проведение испытаний системы.

23. Программно-технические способы и средства обеспечения информационной безопасности
24. Системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов.
25. Оценка эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов.

26. ИБ - риски, специфичные для КВО.

27. Критерии защищенности ИТ- инфраструктуры КВО.

28. Наиболее уязвимые компоненты ИТ - инфраструктуры КВО.

29. Признаки и критерии отнесения систем информационной инфраструктуры к критическим.

Структура и содержание дисциплины
«Безопасность критической информационной инфраструктуры»

10.03.01 «Информационная безопасность» (бакалавр)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Презентация (доклад)	К/р	Э	З
1	**Общая характеристика критически важных объектов РФ** Понятие объекта, критически важного для национальной безопасности государства. Приоритетные направления обеспечения национальной безопасности РФ. Понятия критически важной инфраструктуры, критически важного объекта . Признаки и критерии отнесения систем информационной инфраструктуры к ключевым системам	7	1-3			10	10					+			
2	**Требования по организации**	7	4-6			9	9					+			

	обеспечения безопасности критических информационных инфраструктур. «Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007). «Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 19.11.2007)														
3	**Определение угроз и уровней информационной безопасности критически важных объектов.** Категорирование критически важных объектов в зависимости от негативных последствий, возникающих вследствие прекращения или нарушения их функционирования. Уязвимости критически важных объектов. Причины возникновения уязвимостей. воздействий. Оценка уязвимости критически важных объектов. Степень защищенности критически важных объектов от деструктивного информационного воздействия и актов незаконного вмешательства.	7	7-9			10	10					+			

4	**Разработка требований по обеспечению информационной безопасности критически важных объектов.** Концепция безопасности объекта. Организационные вопросы безопасности. Требования к оформлению концепции обеспечения информационной безопасности объекта. Вопросы безопасности, связанные с персоналом. Требования к классификации и управлению активами, связанными с информационно-телекоммуникационными системами. Вопросы физической защиты и защиты от воздействий окружающей среды. Управление передачей данных и производственной деятельностью. Вопросы защиты от вредоносного программного обеспечения. Контроль доступа к информации и производственным процессам. Порядок разработки и обслуживания систем. Управление непрерывностью производственного процесса. Вопросы безопасности, связанные с радиоэлектронной защитой. Требования безопасности при взаимодействии с открытыми	7	10-12			9	9					+			

	(публичными) информационными системами и сетями. Обеспечение безопасности информационных технологий в ходе эксплуатации информационно-телекоммуникационных систем. Контроль систем на соответствие требованиям. Политика информационной безопасности критически важных объектов. Регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов														
5	**Система защиты информации** Принципы, структурный состав и особенности построения системы защиты информации критически важного объекта. Этапы создания систем защиты информации. Определение информационных и технических ресурсов, подлежащих защите. Выявление полного множества потенциально возможных угроз и каналов утечки информации. Проведение оценки уязвимости и	7	13-15			8	8					+			

	рисков информации при имеющемся множестве угроз и каналов утечки. Определение требований к системе защиты. Осуществление выбора средств защиты информации и их характеристик. Внедрение и организация использования выбранных мер, способов и средств защиты. Осуществление контроля целостности и управление системой защиты.														
6	**Содержание работ по обеспечению безопасности критических информационных инфраструктур** .Выбор средств защиты информации. Анализ отечественного рынка средств защиты информации. Подходы к выбору средств защиты информации. Программно-технические способы и средства обеспечения информационной безопасности. Сертифицированные отечественные средства предупреждения и обнаружения компьютерных атак и защиты информации, разрабатываемые и производимые лицензиатами федеральных органов исполнительной власти. Системы мониторинга средств защиты	7	16-18			8	8					+			

	информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов. Восстановление работоспособности средств защиты информации, функционирующих на критически важных объектах. Оценка эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов.														
7	***Форма аттестации***	7												**Э**	
14	**Всего часов по дисциплине**					**54**	**54**								