МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Институт компьютерных наук и технологий

Авторы-составители: **Карпов Михаил Юрьевич**

Рабочая программа дисциплины

ОРГАНИЗАЦИЯ ЗАЩИТЫ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Код УМК 100620

Утверждено
Протокол №1
от «28» июня 2024 г.

Пермь, 2024

1. Наименование дисциплины

Организация защиты значимых объектов критической информационной инфраструктуры

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в базовую часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.04** Информационно-аналитические системы безопасности
специализация Информационная безопасность финансовых и экономических структур

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Организация защиты значимых объектов критической информационной инфраструктуры** у обучающегося должны быть сформированы следующие компетенции:

10.05.04 Информационно-аналитические системы безопасности (специализация : Информационная безопасность финансовых и экономических структур)

ОПК.11 Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации

Индикаторы

ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем

ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации

4. Объем и содержание дисциплины

Специальность	10.05.04 Информационно-аналитические системы безопасности (специализация: Информационная безопасность финансовых и экономических структур)
форма обучения	очная
№№ семестров, выделенных для изучения дисциплины	9
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	72
Проведение лекционных занятий	36
Проведение практических занятий, семинаров	36
Самостоятельная работа (ак.час.)	72
Формы текущего контроля	Письменное контрольное мероприятие (5)
Формы промежуточной аттестации	Экзамен (9 семестр)

5. Аннотированное описание содержания разделов и тем дисциплины

Система нормативно-правовых актов по вопросам обеспечения безопасности критической информационной инфраструктуры Российской Федерации
Требования профессионального стандарта, предъявляемые к ИТ-специалистам, обеспечивающим защиту компьютерных и автоматизированных объектов информатизации. Подразделение специалистов на категории с указанием уровня компетенций для каждой категории.

Объекты и субъекты критической информационной инфраструктуры (КИИ). Права и обязанности субъектов КИИ. Особенности обеспечения безопасности объектов КИИ. Основные понятия, термины и определения КИИ.
Объекты КИИ в отраслях промышленности. Сферы деятельности в которых определены объекты КИИ. Кто является субъектом КИИ, обязательная аттестация по требованиям безопасности объектов КИИ определенной категории. Понятие информационной системы, автоматизированной системы управления, информационно-телекоммуникационной системы, применительно к объекту КИИ.

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
ГОССОПКА, понятие, задачи, регламентация деятельности, взаимодействие с предприятиями и муниципальными органами, подчиненность.

Система безопасности значимого объекта критической информационной инфраструктуры
Цели и задачи системы безопасности ЗОКИИ, общие требования к созданию систем безопасности различных значимых объектов КИИ. Обеспечение функционирования ЗОКИИ.

Типовые угрозы безопасности информации для информационных систем, информационно-телекоммуникационных систем, автоматизированных систем управления.
Угрозы безопасности информации, реализующиеся через глобальные и региональные автоматизированные сети, через специальное программное обеспечение автоматизированных систем управления. Угрозы безопасности информации реализуемые через средства вычислительной техники. ИТКС

Источники угроз безопасности информации. Уязвимости объектов критической информационной инфраструктуры, классификация уязвимостей. Типовые способы реализации угроз для информационных систем, информационно-телекоммуникационных систем и автом
Внешние и внутренние источники угроз информации. Типичные уязвимости разнообразных объектов КИИ, классификация уязвимостей в зависимости от категорий объектов. Хакерские атаки и иные способы реализации информационных угроз.

Типовые компьютерные инциденты для информационных систем, информационно-телекоммуникационных систем и автоматизированных систем управления.
Компьютерные инциденты, зарубежный и российский опыт атак на критическую инфраструктуру. Российские структуры выявления и пресечения компьютерных атак на отечественную критическую инфраструктуру.

Правила и порядок категорирования объектов критической информационной инфраструктуры. Определение объектов критической информационной инфраструктуры Российской Федерации, которые обрабатывают информацию, необходимую для обеспечения критичес
Категории объектов КИИ Российской Федерации. Правила отнесения и определения объектов КИИ исходя из степени значимости обрабатываемой информации.

Анализ возможных действий нарушителей в отношении объектов критической информационной

инфраструктуры. Оценка возможных последствий компьютерных инцидентов на объектах критической информационной инфраструктуры.
Внешние злоумышленники, внутренние нарушители, критерии оценивания по степени вредоносности применительно к значимым объектам критической информационной инфраструктуры. Подразделение компьютерных инцидентов по степени тяжести применительно к категорированным объектам КИИ.

Организационные и технические меры, направленные на блокирование угроз безопасности информации. Требования к применяемым средствам защиты информации для различных категорий объектов критической информационной инфраструктуры.
Организационно-режимные меры защиты информации, инженерно-физическая защита и техническая защита объектов СВТ и объектов КИИ в целом. Средства защиты информации на объектах информатизации, средства защиты от несанкционированного доступа, средства защиты информации от сетевых атак.

Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования. Организационно-распорядительные документы по безопасности значимых объектов КИИ.
Требования к разработке организационно-распорядительных документов по безопасности ЗОКИИ. Структура системы безопасности ЗОКИИ. Необходимые документы в рамках создания системы безопасности категорированного ЗОКИИ.

Стадии работ по созданию систем безопасности объектов критической информационной инфраструктуры
Этапы жизненного цикла СБ ЗОКИИ. Стадии работ по созданию и тестирование системы безопасности ЗОКИИ. Внедрение системы безопасности. Установка и настройка средств защиты информации. Разработка документов по безопасности ЗОКИИ. Предварительные испытания и опытная эксплуатация ЗОКИИ и его систем безопасности.

Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры.
Мониторинг событий безопасности и контроль за действиями персонала в ЗОКИИ. Внутренний контроль организации работ по обеспечению безопасности ЗОКИИ. Анализ защищенности ЗОКИИ с учетом особенностей его функционирования.

Итоговое мероприятие
Экзамен по курсу: Организация защиты значимых объектов критической информационной инфраструктуры

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Петров, С. В. Информационная безопасность : учебное пособие / С. В. Петров, П. А. Кисляков. — Саратов : Ай Пи Ар Букс, 2015. — 326 с. — ISBN 978-5-906-17271-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/33857

2. Технические средства и методы защиты информации:учебное пособие для студентов вузов, обучающихся по специальностям 090102 "Компьютерная безопасность",090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем"/А. П. Зайцев [и др.] ; ред.: А. П. Зайцев, А. А. Шелупанов.-4-е изд., испр. и доп..-Москва:Горячая линия - Телеком,2012, ISBN 978-5-9912-0084-4.-616.-Библиогр.: с. 608-609

Дополнительная:

1. Информатика. Часть 2. Программно-технические средства : учебно-методический комплекс дисциплины по направлению подготовки 51.03.06 (071900.62) «Библиотечно-информационная деятельность», профили подготовки: «Информационно-аналитическая деятельность», «Технология автоматизированных библиотечно-информационных систем», квалификация «бакалавр» / составители Г. Ф. Леонидова. — Кемерово : Кемеровский государственный институт культуры, 2014. — 84 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/55228.html

2. Технические средства и методы защиты информации:учебное пособие для студентов вузов, обучающихся по специальностям 090102 "Компьютерная безопасность",090105 "Комплексное обеспечение информационной безопасности автоматизированных систем", 090106 "Информационная безопасность телекоммуникационных систем"/А. П. Зайцев [и др.] ; ред.: А. П. Зайцев, А. А. Шелупанов.-4-е изд., испр. и доп..-Москва:Горячая линия - Телеком,2012, ISBN 978-5-9912-0084-4.-616.-Библиогр.: с. 608-609

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

При освоении дисциплины использование ресурсов сети Интернет не предусмотрено.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Организация защиты значимых объектов критической информационной инфраструктуры** предполагает использование следующего программного обеспечения и информационных справочных систем:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета.

1. Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC»;
- офисный пакет приложений «LibreOffice», Alt Linux;
- Специализированное программное обеспечение Специализированного учебного кабинета «Лаборатория программно-аппаратных средств» (защищённое помещение по конфиденциальной информации).

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

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

Для лекционных занятий требуется аудитория, оснащенная специализированной мебелью, презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.

Для проведения семинарских (практических) занятий - Специализированный учебный кабинет «Лаборатория программно-аппаратных средств» (защищённое помещение по конфиденциальной информации) со специализированным оборудованием и программным обеспечением.

Для групповых (индивидуальных) консультаций, текущего контроля и промежуточной аттестации - Аудитория, оснащенная: специализированной мебелью, проектором, ноутбуком/компьютером, экраном, маркерной или меловой доской.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Организация защиты значимых объектов критической информационной инфраструктуры

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ОПК.11

Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Знает типовые уязвимости значимых объектов КИИ. Может предложить решение по защите информации.	**Неудовлетворител** Знает менее 50% основных требований при решении учебно-теоретических и практических задач в области защиты информации; Не умеет применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Не владеет основными навыками работы со средствами защиты информации. **Удовлетворительн** Знает не менее 50% основных требований при решении учебно-теоретических и практических задач в области защиты информации; Умеет (с ошибками) применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Не владеет основными навыками работы со средствами защиты информации. **Хорошо** Знает не менее 70% основных требований при решении учебно-теоретических и практических задач в области защиты информации; Умеет применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Владеет (с ошибками) основными навыками работы со средствами защиты информации. **Отлично** Знает основные требования при решении

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично учебно-теоретических и практических задач в области защиты информации; Отлично умеет применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Владеет навыками работы со средствами защиты информации.
ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Умеет контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем. Знает основные методы политик безопасности АС. Может применить практически.	**Неудовлетворител** Знает менее 50% основных требований при решении учебно-теоретических и практических задач в области защиты информации; Не умеет применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Не владеет основными навыками работы со средствами защиты информации. **Удовлетворительн** Знает не менее 50% основных требований при решении учебно-теоретических и практических задач в области защиты информации; Умеет (с ошибками) применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Не владеет основными навыками работы со средствами защиты информации. **Хорошо** Знает не менее 70% основных требований при решении учебно-теоретических и практических задач в области защиты информации; Умеет применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Владеет (с ошибками) основными навыками работы со средствами защиты информации. **Отлично** Знает основные требования при решении

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично учебно-теоретических и практических задач в области защиты информации; Отлично умеет применять современные теоретические и экспериментальные методы исследования компьютерных систем по требованиям информационной безопасности; Владеет навыками работы со средствами защиты информации.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Экзамен
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 41 до 60
«неудовлетворительно» / «незачтено» менее 41 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Система безопасности значимого объекта критической информационной инфраструктуры **Письменное контрольное мероприятие**	Определяет цели и задачи системы безопасности ЗОКИИ, классифицирует требования к созданию систем безопасности различных значимых объектов КИИ. Обеспечивает функционирование ЗОКИИ.
ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Типовые компьютерные инциденты для информационных систем, информационно - телекоммуникационных систем и автоматизированных систем управления. **Письменное контрольное мероприятие**	Умеет определять компьютерные инциденты, анализирует опыт атак на критическую инфраструктуру. , Классифицирует уязвимости. Определяет типовые способы реализации угроз для ИС, ИТКС, АСУ.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
	Организационные и технические меры, направленные на блокирование угроз безопасности информации. Требования к применяемым средствам защиты информации для различных категорий объектов критической информационной инфраструктуры. **Письменное контрольное мероприятие**	Знает порядок категорирования объектов КИИ. Определяет объекты КИИ РФ, которые обрабатывают информацию, необходимую для обеспечения критических процессов. Проводит анализ возможных действий нарушителей в отношении объектов КИИ. Проводит оценку возможных последствий инцидентов на объектах КИИ РФ.
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации **ОПК.11.1** Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры. **Письменное контрольное мероприятие**	Определяет стадии работ по созданию систем безопасности. Обеспечивает контроль за безопасностью значимого объекта КИИ.
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Итоговое мероприятие **Письменное контрольное мероприятие**	Выполняет анализ и оценку защищенности выбранного объекта как объекта критической информационной инфраструктуры. Проводит все необходимые процедуры по аттестации объекта по требованиям действующих нормативных документов ФСТЭК России и представляет в виде пакета документов (в электронном виде) подтверждающих создание системы безопасности объекта КИИ.

Спецификация мероприятий текущего контроля

Система безопасности значимого объекта критической информационной инфраструктуры

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **8.2**

Показатели оценивания	Баллы
Знает не менее 70% основных сведений о теории и практике развития информационной безопасности в РФЗнает не менее 80% требований профессионального стандарта к специалисту в области безопасности автоматизированных систем и компьютерных сетей. Имеет четкое представление об особенностях обеспечения информационной безопасности в системе национальной безопасности Российской Федерации, структуре системы информационной безопасности.Имеет представления о методиках поиска конкретизированной информации в различных системах.Может грамотно проводить анализ, структурирование и заключение по найденной информации.Может правильно оформить и представить результаты поиска информации. Умеет работать в команде.	11.8
Знает общие сведения о теории и практике развития информационной безопасности в РФ Знает не менее 50% требований профессионального стандарта к специалисту в области безопасности автоматизированных систем.Имеет представление об особенностях обеспечения информационной безопасности в системе национальной безопасности Российской федерацииНе имеет представления о методиках поиска конкретизированной информацииНе может проводить анализ, структурирование и заключение по найденной информацииНе может правильно оформить и представить результаты поиска информации. Не умеет работать в команде.	8.2

Типовые компьютерные инциденты для информационных систем, информационно - телекоммуникационных систем и автоматизированных систем управления.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **8.2**

Показатели оценивания	Баллы
Знает не менее 70% основных критериев отнесения информации к критически важной. Знает не менее 70% отраслей промышленности и структур государства критичных к информационному воздействию.Знает объекты КИИ, наиболее подверженные информационным атакам.Знает не менее 70% основных требований при взаимодействии гражданских структур с ГОСОПКа. Знает детально, что такое компьютерные инциденты. Знает типовые угрозы объектам КИИ.Умеет правильно оценивать информационное воздействие на критическую инфраструктуру, его последствия.Может выстроить (теоретически) правильные модели защиты разнообразных автоматизированных систем от внешнего информационного воздействия.	11.8
Знает не менее 50% основных критериев отнесения информации к критически важной.	8.2

Знает не менее 50% отраслей промышленности и структур государства критичных к информационному воздействию.Знает в общих чертах объекты КИИ, наиболее подверженные информационным атакам.Знает не менее 50% основных требований при взаимодействии гражданских структур с ГОСОПКа. Знает в общих чертах что такое компьютерные инциденты.Не умеет правильно оценивать информационное воздействие на критическую инфраструктуруНе может выстроить (теоретически) модель защиты автоматизированной системы от внешнего информационного воздействия.	

Организационные и технические меры, направленные на блокирование угроз безопасности информации. Требования к применяемым средствам защиты информации для различных категорий объектов критической информационной инфраструктуры.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **8.2**

Показатели оценивания	Баллы
Знает не менее 70% основных нормативно-методических документов ФСТЭК России по безопасности критической информационной инфраструктуры.Знает не менее 80% основных понятий и терминов в области информационной безопасности, безопасности критической информационной инфраструктуры, автоматизированных систем обработки информации.Знает хорошо принципы организации хакерских атак на различные информационные системы. Умеет анализировать действия нарушителей, оценивать последствия воздействий.Умеет оценить результаты и полноту выполненных работ по заданной теме.Может оформить и представить результаты выполненных работ по тематике информационного воздействия.	11.8
Знает не менее 50% основных нормативно-методических документов ФСТЭК России по безопасности критической информационной инфраструктуры.Знает не менее 50% основных понятий и термины в области информационной безопасности, безопасности критической информационной инфраструктуры, автоматизированных систем обработки информации.Знает частично принципы организации хакерских атак на различные информационные системы. Не умеет правильно анализировать действия нарушителей и последствия компьютерных инцидентов.Умеет приблизительно оценить результаты и полноту выполненных работ по заданной теме.Может с некритичными ошибками оформить и представить результаты выполненных работ по тематике информационного воздействия.	8.2

Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **8.2**

Показатели оценивания	Баллы
Знает не менее 70% основных нормативно-методических документов ФСТЭК России по безопасности критической информационной инфраструктуры.Знает не менее 80% основных понятий и термины в области информационной безопасности, безопасности критической информационной инфраструктуры, автоматизированных систем обработки информации.Знает принципы создания организационно-распорядительных документов для различных информационных систем КИИ. Знает этапы создания систем безопасности объектов КИИ.Умеет в полном объеме оценить результаты контроля защищенности объекта КИИ и полноту выполненных работ по заданной теме. Может оформить и представить результаты выполненных работ по тематике информационного воздействия. Может выполнить учебно-практическую задачу по моделированию системы безопасности значимого объекта КИИ.	11.8
Знает не менее 50% основных нормативно-методических документов ФСТЭК России по безопасности критической информационной инфраструктуры.Знает не менее 50% основных понятий и термины в области информационной безопасности, безопасности критической информационной инфраструктуры, автоматизированных систем обработки информации.Знает частично принципы создания организационно-распорядительных документов для различных информационных систем. Знает в общих чертах этапы создания систем безопасности объектов КИИ.Умеет приблизительно оценить результаты контроля защищенности объекта КИИ и полноту выполненных работ по заданной теме.Может с некритичными ошибками оформить и представить результаты выполненных работ по тематике информационного воздействия.	8.2

Итоговое мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **8.2**

Показатели оценивания	Баллы
Знает сведения о теории и практике развития системы защиты значимых объектов критической информационной инфраструктуры в РФ. Знает не менее 70% нормативных документов ФСТЭК РФ по обеспечению защиты информации на объектах КИИ.Знает не менее 80% требований профессионального стандарта к специалисту в области безопасности автоматизированных систем. Знает правила создания организационно-распорядительных и технических документов для объектов КИИ.Знает особенности обеспечения информационной безопасности в системе значимых объектов КИИ Российской федерации.Знает методики создания иерархической системы защиты объектов КИИ.Может проводить анализ, структурирование и заключение по созданию системы безопасности значимого объекта КИИ, комплекса объектов КИИ.Может оформить и представить результаты анализа уязвимостей объекта КИИ, выполнить моделирование	11.8

системы защиты с использованием организационных и технических средств и мер защиты..	
Знает общие сведения о теории и практике развития системы защиты значимых объектов критической информационной инфраструктуры в РФ. Знает не менее 50% нормативных документов ФСТЭК РФ по обеспечению защиты информации на объектах КИИ. Знает не менее 50% требований профессионального стандарта к специалисту в области безопасности автоматизированных систем. Знает общие правила создания организационно-распорядительных документов для объектов КИИ.Имеет представление об особенностях обеспечения информационной безопасности в системе значимых объектов КИИ Российской федерацииИмеет общее представления о методиках создания иерархической системы защиты объектов КИИ.Может обобщенно проводить анализ, структурирование и заключение по созданию системы безопасности значимого объекта КИИ, комплекса объектов КИИ.Может обобщенно оформить и представить результаты анализа уязвимостей объекта КИИ, выполнить моделирование системы защиты с использованием организационных и технических средств и мер защиты..	8.2