

Аннотации дисциплины

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Петренко Вячеслав Иванович

Должность: и.о. директора Института цифрового развития

Дата подписания: 27.07.2024 16:03:15

Уникальный программный ключ:

b47f96eea65a16e179f94dbf7fb0b10000e7ad4d

Наименование дисциплины	Защита объектов критической информационной инфраструктуры
Краткое содержание	Основные понятия и определения изучаемой дисциплины. Правовые основы обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Организационно-правовые основы аттестации значимых объектов КИИ, лицензирования деятельности в области защиты информации. Система сертификации средств защиты информации. Угрозы безопасности информации, обрабатываемой на объектах КИИ. Источники угроз безопасности информации. Уязвимости объектов КИИ, классификация уязвимостей. Способы реализации угроз безопасности информации и их последствия. Банк данных угроз безопасности информации. Структура модели угроз безопасности информации значимого объекта КИИ. Категорирование объектов КИИ. Реестр значимых объектов КИИ. Перечень показателей критериев значимости объектов КИИ Российской Федерации и их значения. Требования по обеспечению безопасности значимых объектов КИИ. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов КИИ. Требования к классам защиты средств защиты информации и средствам вычислительной техники для различных категорий значимости объектов КИИ. Система безопасности значимого объекта КИИ. Стадии (этапы) работ по созданию систем безопасности значимого объекта КИИ. Контроль за обеспечением безопасности значимого объекта КИИ.
Результаты освоения дисциплины	- определяет категории значимости объектов КИИ; - определяет требования к обеспечению безопасности значимого объекта КИИ; - разрабатывает модели угроз безопасности информации значимых объектов КИИ; - обосновывает организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта КИИ; - разрабатывает архитектуру системы безопасности значимого объекта КИИ; - осуществляет выбор средств защиты информации с учетом категории значимости объекта КИИ; - определяет требования к параметрам настройки программных и программно-аппаратных средств.
Трудоемкость, з.е.	3 з.е.
Формы отчетности	Зачет с оценкой – 5 семестр
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: учебное пособие. В 2-х ч. Ч. 1. Правовое обеспечение информационной безопасности. - М.: МИЭТ, 2013. - 184 с.

	2. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: учебное пособие. В 2-х ч. Ч. 2. Организационное обеспечение информационной безопасности. - М.: МИЭТ, 2013.- 172 с. 3. Мельников В.В. Безопасность информации в автоматизированных системах. - М.: Финансы и статистика, 2003. – 368 с. 4. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: учебное пособие для вузов. - М.: Радио и связь, 2000. – 168 с.
Дополнительная литература	1. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». 2. Федеральный закон от 26.07.2017 г. № 193-ФЗ «О внесении изменений в отдельные законодательные акты РФ в связи с принятием ФЗ «О безопасности КИИ РФ». 3. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности КИИ РФ». 4. Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утверждены постановлением Правительства Российской Федерации от 17 февраля 2018 г. № 162. 5. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений. Утверждены постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 (ред. от 20.12.2022). 6. Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации. Утвержден приказом ФСТЭК России от 6 декабря 2017 г. № 227. 7. Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования. Утверждены приказом ФСТЭК России от 21 декабря 2017 г. № 235. 8. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утверждены приказом ФСТЭК России от 25 декабря 2017 г. №239 (в ред. приказа ФСТЭК России от 9 августа 2018 г. № 138). 9. Методический документ. Методика оценки угроз безопасности информации. Утверждена ФСТЭК России 5 февраля 2021 г.