Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Институт информационных технологий и анализа данных»

УТВЕРЖДЕНА:
на заседании Совета института ИТиАД им. Е.И.Попова
Протокол №8 от 24 февраля 2025 г.

Рабочая программа дисциплины

«РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление: 10.03.01 Информационная безопасность

Организация и технологии защиты информации (в сфере техники и технологии)

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Мамедов Эльшан Фахраддинович Дата подписания: 17.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 17.06.2025	Документ подписан простой электронной подписью Согласовал: Сибиряк Юрий Владимирович Дата подписания: 18.06.2025

Год набора – 2025

Иркутск, 2025 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Реагирование на инциденты информационной безопасности» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ДК-1 Способность осуществлять деятельность, находящуюся за пределами основной профессиональной сферы	ДК-1.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ДК-1.2	Знает комплекс мер по реагированию на инциденты в сфере информационных и компьютерных технологий. Может определить основные стадий: обнаружение и регистрация компьютерных инцидентов, реагирование на компьютерные инциденты, и анализ результатов деятельности по управлению компьютерными инцидентами	**Знать** нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов критической информационной инфраструктуры; основы функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы российской федерации; основные понятия в области обеспечения безопасности информации, обрабатываемой объектами критической информационной инфраструктуры; принципы организации систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечения их функционирования; процедуру категорирования объектов критической информационной инфраструктуры, в том числе порядок создания комиссии по категорированию, порядок определения категорий значимости объектов критической информационной инфраструктуры; процедуру подготовки и направления в фстэк россии сведений о результатах присвоения объекту критической

		информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий; основные принципы выявления наличия критических процессов у субъекта критической информационной инфраструктуры; основные принципы выявления объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов; процедуры выявления и анализа угроз безопасности информации, обрабатываемой объектом критической информационной инфраструктуры; общие требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры; общие требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации обеспечению их функционирования; требования к правовым, организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов кии; требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры; цели, задачи, основные принципы организации государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры; порядок обработки результатов контроля (проверки) состояния безопасности значимых объектов критической информационной инфраструктуры; роль

		защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак **Уметь** формировать сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий; выявлять и анализировать угрозы безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта критической информационной инфраструктуры, возможных способов реализации угроз безопасности и последствий от их реализации; обосновывать организационные и технические меры, подлежащие реализации в рамках системы безопасности значимого объекта критической информационной инфраструктуры; определять структуру системы безопасности значимого объекта критической информационной инфраструктуры; осуществлять выбор средств защиты информации с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта критической информационной инфраструктуры; определять требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности

		информации; определять требования к обеспечению безопасности значимого объекта критической информационной инфраструктуры; определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер в рамках системы безопасности значимого объекта критической информационной инфраструктуры; определять структуру системы безопасности значимого объекта критической информационной инфраструктуры; осуществлять выбор средств защиты информации с учетом их стоимости, совместимости с применяемыми программными и программно-аппаратными средствами, функций безопасности этих средств и особенностей их реализации, а также категории значимого объекта критической информационной инфраструктуры; определять требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации; определять требования к обеспечению безопасности значимого объекта критической информационной инфраструктуры; применять программные и (или) программно-аппаратные средства на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов **Владеть** навыками работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

		навыками работы с базами данных, содержащими информацию по угрозам безопасности информации и уязвимостям программного обеспечения значимых объектов критической информационной инфраструктуры, в том числе зарубежными информационными ресурсами; навыками разработки организационно-распорядительных документов по безопасности значимых объектов критической информационной инфраструктуры; эксплуатации системы безопасности значимого объекта критической информационной инфраструктуры; навыками выявления угроз безопасности информации по результатам оценки возможностей внешних и внутренних нарушителей, анализа потенциальных уязвимостей значимого объекта критической информационной инфраструктуры; навыками участия в разработке организационных и технических мероприятий по защите объектов критической информационной инфраструктуры; навыками установки, настройки и применения современных средств защиты информации, обрабатываемой объектами критической информационной инфраструктуры; навыками проведения работ по контролю состояния безопасности объектов критической информационной инфраструктуры; навыками работы с информационными системами, информационно-телекоммуникационными сетями, автоматизированными системами управления субъектов критической информационной инфраструктуры

2 Место дисциплины в структуре ООП

Изучение дисциплины «Реагирование на инциденты информационной безопасности» базируется на результатах освоения следующих дисциплин/практик: «Аудит информационной безопасности», «Основы информационной безопасности»,

«Персональные данные», «Организационное и правовое обеспечение информационной безопасности»

Дисциплина является предшествующей для дисциплин/практик: «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Нормативная база, российские и международные стандарты по информационной безопасности», «Основы управления информационной безопасностью»

3 Объем дисциплины

Объем дисциплины составляет – 3 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 6
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	48	48
лекции	32	32
лабораторные работы	0	0
практические/семинарские занятия	16	16
Самостоятельная работа (в т.ч. курсовое проектирование)	60	60
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет	Зачет

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 6

№ п/п	Наименование раздела и темы дисциплины	Виды контактной работы						СРС		Форма текущего контроля
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Основы обеспечения безопасности КИИ Российской Федерации	1	3							Устный опрос
2	Правовое обеспечение критической информационной инфраструктуры	2	3			1	2	2	10	Устный опрос
3	Категорирование объектов критической информационной инфраструктуры	3	3							Устный опрос
4	Обеспечение	4	3			2	2	2	10	Устный

	безопасности значимых объектов критической информационной инфраструктуры									опрос
5	Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры	5	3			3	4			Устный опрос
6	Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры.	6	6					1	20	Устный опрос
7	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)	7	6			4	4	2	10	Устный опрос
8	Аудит безопасности критической инфраструктуры	8	5			5	4	2	10	Устный опрос
	Промежуточная аттестация									Зачет
	Всего		32				16		60	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 6

№	Тема	Краткое содержание
1	Основы обеспечения безопасности КИИ Российской Федерации	Введение в безопасность объектов критической информационной инфраструктуры. Термины и определения, понятие критической информационной инфраструктуры. Полномочия органов государственной власти Российской Федерации в области обеспечения безопасности КИИ.
2	Правовое обеспечение критической	Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной

	информационной инфраструктуры	инфраструктуры Российской Федерации". Указы Президента РФ. Постановления Правительства РФ. Приказы ФСТЭК России и ФСБ России. Оценка безопасности критической информационной инфраструктуры. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.
3	Категорирование объектов критической информационной инфраструктуры	Объекты и субъекты критической информационной инфраструктуры. Правила категорирования объектов критической информационной инфраструктуры. Общий порядок работ. Критерии значимости объектов критической информационной инфраструктуры. Подготовка исходных данных для категорирования объектов критической информационной инфраструктуры. Определение принадлежности к субъектам критической информационной инфраструктуры. Создание комиссии по категорированию. Формирование перечня критических процессов. Формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию. Категорирование объектов критической информационной инфраструктуры. Анализ возможных источников угроз и действий предполагаемых нарушителей. Угрозы безопасности информации объекта КИИ. Построение модели угроз и нарушителей объектов КИИ. Процедуры выявленияи анализа угроз безопасности информации, обрабатываемой объектом КИИ. Оценка масштаба последствий и соотнесение со значениями показателей категорий. Определение категории значимости объекта КИИ. Оформление и передача в ФСТЭК России результатов категорирования. Внесение изменений в результаты категорирования. Подготовка отчетных документов и контроль результатов категорирования объектов КИИ.
4	Обеспечение безопасности значимых объектов критической информационной инфраструктуры	Требований по обеспечению безопасности значимых объектов КИИ РФ. Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности

		информации. Система безопасности значимого объекта КИИ. Порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Стадии (этапы) работ по созданию систем безопасности объекта КИИ. Требования к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования. Разработка организационно-распорядительных документов по безопасности значимых объектов КИИ.
5	Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры	Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ. Правила организации повышения квалификации специалистов по защите информации и должностных лиц, ответственных за организацию защиты информации в органах государственной власти, органах местного самоуправления, организациях с госучастием и организациях оборонно-промышленного комплекса. Порядок ведения реестра значимых объектов КИИ РФ. Итоги проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ. Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и порядок получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения. Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ.
6	Организационно-распорядительные документы по обеспечению безопасности значимых объектов критической информационной инфраструктуры.	Организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила обеспечения безопасности значимых объектов КИИ, определяющие порядок и правила функционирования системы безопасности значимых объектов КИИ.
7	Государственная	Перечень информации, представляемой в

	система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)	ГосСОПКА и Порядок представления информации в ГосСОПКА. О Национальном координационном центре по компьютерным инцидентам (НКЦКИ).
8	Аудит безопасности критической инфраструктуры	Аудит критической информационной инфраструктуры. Особенности проведения аудита критической информационной инфраструктуры. Определение аудита информационной безопасности. Цели и задачи аудита. Этапы проведения аудита. Схема проведения аудита. Общие подходы к проведению аудита. Классификация аудита. Результаты аудита объектов критической информационной инфраструктуры. Тестирование как один из основных типов аудита критической информационной инфраструктуры. Тестирование: определение, требования, классификация. Тестирование на основе моделей. Тестирование специальными средствами и способами информационных воздействий. Особенности тестирования критической инфраструктуры информационными воздействиями в технической и в психологических сферах. Тестирование критической инфраструктуры специальными информационно-техническими воздействиями. Общая классификация информационно-технических воздействий. Оборонительные информационно-технические воздействия. Обеспечивающие информационно-технические воздействия. Атакующие информационно-технические воздействия. Классификация основных средств информационно-технических воздействий.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 6

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Правовое обеспечение критической информационной инфраструктуры	2
2	Обеспечение безопасности значимых объектов	2

	критической информационной инфраструктуры	
3	Контроль за обеспечением безопасности значимого объекта критической информационной инфраструктуры	4
4	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)	4
5	Аудит безопасности критической инфраструктуры	4

4.5 Самостоятельная работа

Семестр № 6

№	Вид СРС	Кол-во академических часов
1	Подготовка к зачёту	20
2	Подготовка к практическим занятиям (лабораторным работам)	40

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Дискуссия, Кейс-технология

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

https://el.istu.edu/course/index.php?categoryid=1107

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/course/index.php?categoryid=1107

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 6 | Устный опрос

Описание процедуры.

Тема 3. Категорирование объектов критической информационной инфраструктуры.
Описание процедуры:
Проведение устного опроса в форме «вопрос-ответ»
Вопросы для контроля:
1. Правила категорирования объектов критической информационной инфраструктуры;
2. Создание комиссии по категорированию;
3. Угрозы безопасности информации объекта КИИ.

Критерии оценивания.

Полнота ответа: Раскрытие всех аспектов вопроса, использование ключевых понятий, терминов.
Точность и достоверность: Правильность определений, формул, фактов, дат, имен, ссылок на источники.
Глубина понимания: Демонстрация понимания сути явлений, причинно-следственных связей, умение анализировать, синтезировать, обобщать, а не просто воспроизводить заученное.
Логичность и структурированность: Последовательность изложения, наличие введения, основной части, вывода.
Культура речи: Грамотность, ясность, использование профессиональной терминологии.
Умение аргументировать: Подтверждение своих тезисов примерами, доказательствами, ссылками на теории.
Ответы на дополнительные/уточняющие вопросы: Способность развить тему, применить знания в нестандартной ситуации.

ответ раскрыт полностью – 5 баллов
ответ раскрыт частично – 2-4 баллов
имеет только общее представление о проблеме – 1 балл
не ответил – 0 баллов

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	Критерии оценивания	Средства (методы) оценивания промежуточной аттестации
ДК-1.2	Способен применять нормативные правовые акты, методические документы и национальные стандарты в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. применять программные и (или) программно-аппаратные средства на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов. Показывает навыки работы с нормативными правовыми актами, методическими документами в области обеспечения безопасности значимых объектов критической информационной инфраструктуры. Показывает навыки работы с информационными системами, информационно-телекоммуникационными сетями,	Тестовые задания зачет

	автоматизированными системами управления субъектов критической информационной инфраструктуры.	

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 6, Типовые оценочные средства для проведения зачета по дисциплине

6.2.2.1.1 Описание процедуры

Перечень теоретических вопросов, практических заданий и ситуаций, выносимых на зачет, доводятся преподавателем до студентов в начале изучения программы. Формулировки вопросов, заданий должны быть четкими, краткими, понятными, исключающими двойное толкование. Могут быть применены тестовые задания или задания комбинированного характера. Количество вариантов для устных заданий должно быть больше чем число студентов, сдающих зачет не менее, чем на 3. Количество вариантов для письменных заданий должно быть не менее двух.

Перечень примерных вопросов для зачета
1. Понятие инцидентов ИБ.
2. Нормативная база в сфере управления инцидентами ИБ.
3. Система управления инцидентами ИБ.
4. Обработка событий и инцидентов ИБ.
5. Реагирование на инциденты ИБ.
6. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ.
7. Сбор технических данных с компонентов информационной инфраструктуры.
8. Поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформлению.
9. Распространение (передача) выделенной и оформленной содержательной (семантической) информации.
10. Обеспечение наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры.
11. Сбор и фиксация информации об инцидентах ИБ.
12. Проверка целостности (неизменности) собранных данных, маркирование носителей собранных данных.
13. Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования.
14. Копирование содержимого оперативной памяти СВТ и получение данных операционных систем.
15. Копирование протоколов (журналов) регистрации.
16. Копирование сетевого трафика.
17. Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление.
18. Структура протокола обработки технических данных.
19. Технические средства и инструменты для сбора и обработки технических данных.
20. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).
21. Ответственность за невыполнение требований по реагированию на компьютерные

инциденты.

Пример задания:

1. Какой документ регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак?

a) Федеральный закон от 26.07.2017 № 187ФЗ;
b) Приказ ФСБ России от 19.06.2019 № 281;
c) Приказ ФСТЭК России от 25 декабря 2017 г. № 239;
d) Постановление Правительства РФ от 8 февраля 2018 г. № 127.

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено
Ответ правильный, логически выстроен, использована профессиональная терминология. Обучающийся правильно интерпретирует полученный результат.	Ответы неправильные или неполные.

7 Основная учебная литература

1. Рудаков А. В. Операционные системы и среды [Электронный ресурс] : учебник / А. В. Рудаков, 2022. - 304.

2. Батаев А. В. Операционные системы и среды : учебник для студентов среднего специального образования / А. В. Батаев, Н. Ю. Налютин, С. В. Синицин, 2021. - 288.

3. Прохорова О. В. Информационная безопасность и защита информации / О. В. Прохорова, 2023. - 124.

4. Усов Е. Г. Защита информации : электронный курс / Е. Г. Усов, 2023

5. Методические указания по проведению лабораторных работ по дисциплине "Техническая защита информации" по теме "Защита информации от утечки по цепям электропитания" [Электронный ресурс] : для студентов по направлению подготовки/специальности 10.03.01 "Информационная безопасность" / Иркут. нац. исслед. техн. ун-т, Ин-т высоких технологий, Каф. информ. безопасности, 2018. - 30.

6. Внуков А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры по инженерно-техническим направлениям / А. А. Внуков, 2017. - 245.

8 Дополнительная учебная литература и справочная

1. Левин Максим. E-mail "безопасная": взлом, "спам" и "хакерские" атаки на системы электронной почты Internet / Максим Левин, 2002. - 189.

2. Леонтьев Борис Константинович. Хакеры, взломщики и другие информационные убийцы : [Для систем. администраторов] / Борис Леонтьев, 2002. - 190.

3. Белоус А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха, 2020. - 692.

4. Ховард Р. Кибербезопасность: главные принципы / Р. Ховард, 2024. - 320.

5. Белоус А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства / А. И. Белоус, 2020. - 644.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Microsoft DreamSpark Premium Electronic Software Delivery_2018

2. Microsoft Office 2007 Standard - 2003 Suites и 2007 Suites - поставка 2010

12 Материально-техническое обеспечение дисциплины

1. Проектор мультимедиа BenQ MW621ST(с экраном 3*3 м)

2. Экран ScreenMedia GoldView 274*206 настенный