МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Казанский национальный исследовательский
технологический университет»
(ФГБОУ ВО «КНИТУ»)

УТВЕРЖДАЮ
Проректор по учебной работе
Д.Ш. Султанова
«07» июня 2021 г.

Рабочая программа дисциплины в виде электронного документа выгружена из информационной системы управления университетом и соответствует оригиналу
Простая электронная подпись, ID подписи: 1060
Подписал Проректор по учебной работе Д.Ш. Султанова
Дата 07.06.2021

РАБОЧАЯ ПРОГРАММА
по дисциплине **«АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОКОММУНИКАЦИЙ»**

Направление подготовки:	10.03.01 Информационная безопасность
Профиль:	Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника:	Бакалавр
Форма обучения:	Очно-заочная
Институт:	Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия"
Факультет:	Инжиниринговый центр в области химии и технологии энергонасыщенных материалов"Спецхимия"
Кафедра-разработчик:	Казанский межвузовский инженерный центр "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет"
Курс; семестр	4; 8

Вид нагрузки	Часы	Зачётные единицы
Лекция	18	0,5
Лабораторная работа	36	1
Практическое занятие	18	0,5
Контроль самостоятельной работы	54	1,5
Самостоятельная работа	63	1,75
Форма аттестации: Экзамен (8 сем)	27	0,75
Всего	216	6

Казань, 2021

Рабочая программа составлена с учётом требований Федерального государственного образовательного стандарта (приказ № 1427 от 17.11.2020) по направлению подготовки 10.03.01 Информационная безопасность для профиля «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» на основании учебных планов набора обучающихся 2021 года.

Разработчик программы:

Доцент А.Ю. Сенцова

С О Г Л А С О В А Н О

Рабочая программа рассмотрена и одобрена на заседании Казанского межвузовского инженерного центра "Новые технологии" федерального государственного бюджетного образовательного учреждения высшего образования "Казанский национальный исследовательский технологический университет", протокол от 19.05.2021 г. № 6.

Директор ***Согласовано*** А.Ф. Махоткин

У Т В Е Р Ж Д Е Н О

Начальник центра УМЦ ***Утверждаю*** Л.А. Китаева

1. Цели освоения дисциплины

Целями освоения дисциплины «Аудит информационной безопасности объектов инфокоммуникаций» являются:

-освоение теоретических основ и изучение принципов проведения аудита информационной безопасности, теоретических основ лицензирования и сертификации деятельности в области защиты информации;

-ознакомление с методами и средствами проведения аудита информационной безопасности объектов;

-приобретение практических навыков проведения аудита информационной безопасности;

-формирование у студентов умения проводить комплексные проверки информационной безопасности объектов.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Аудит информационной безопасности объектов инфокоммуникаций» относится к обязательной части ООП и формирует у обучающихся по профилю «Безопасность телекоммуникационных систем (по отрасли или в сфере профессиональной деятельности)» набор знаний, умений, навыков и компетенций.

Для успешного освоения дисциплины «Аудит информационной безопасности объектов инфокоммуникаций» обучающийся по направлению подготовки 10.03.01 «Информационная безопасность» должен освоить материал предшествующих дисциплин:

1. Защита информационных процессов в телекоммуникациях
2. Информационные технологии в информационной безопасности
3. Организационное и правовое обеспечение информационной безопасности
4. Основы информационной безопасности
5. Теория информации

Дисциплина «Аудит информационной безопасности объектов инфокоммуникаций» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Аудит информационной безопасности объектов инфокоммуникаций
2. Проектирование защищенных телекоммуникационных систем
3. Производственная практика (технологическая практика)

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ОПК-5.2 Способен применять технологии защиты информации при создании защищенных телекоммуникационных систем;

ОПК-5.2.1. Знает современные законы, стандарты, методы и технологии в области защиты информации

ОПК-5.2.2. Умеет использовать современные программно-аппаратные средства защиты информации при создании защищенных телекоммуникационных систем

ОПК-5.2.3. Владеет современными методами и технологиями обеспечения защиты информации при создании защищенных телекоммуникационных систем

ОПК-5.4 Способен проводить мониторинг функционирования защищенных телекоммуникационных систем;

ОПК-5.4.1. Знает порядок проведения мониторинга функционирования защищенных телекоммуникационных систем

ОПК-5.4.2. Умеет проводить мониторинг и анализ защищенности информации от несанкционированного доступа в телекоммуникационных системах в целях управления их функционированием

ОПК-5.4.3. Владеет способностью проводить мониторинг функционирования защищенных телекоммуникационных систем

В результате освоения дисциплины обучающийся должен

Знать:

-принципы и методы организационной защиты информации; принципы и методы

организационной защиты информации; о мерах по поддержанию в работоспособном состоянии ОС; методы установки, настройки и обслуживания технических и программно-аппаратных средств защиты информации;

-технологии и нормы обеспечения информационной безопасности телекоммуникационных систем;

Уметь:

-обеспечивать защиту информации при создании защищенных телекоммуникационных систем;

-пользоваться нормативными документами по защите информации; определять условия функционирования ОС; производить установку, настройку и обслуживание технических и программно-аппаратных средств защиты информации;

Владеть:

-методами технической защиты информации; методами и средствами, в том числе автоматизированными, установки, настройки и обслуживания технических и программно-аппаратных средств защиты информации;

-способами практического обеспечения норм информационной безопасности при создании защищенных телекоммуникационных систем;

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 6 зачетных единиц, 216 часов.

№ п/п	Раздел дисциплины	Семе-стр	Виды учебной работы (в часах)					Оценочные средства для проведения текущей и промежу-точной аттестации
			Лекция	Практические занятия	Лабора-торные	КСР	СРС	
1	2	3	4	5	6	7	8	9
1.	Теоретические основы применения аудита информационной безопасности объектов (информационных технологий и систем обеспечения информационной безопасности)	8	10	18		24	28	Практические занятия; Реферат; Экзамен
2.	Методика проведения аудита информационной безопасности информационных технологий и систем обеспечения информационной безопасности. Лицензирование и сертификация деятельности в	8	8		36	30	35	Лабораторная работа; Реферат; Экзамен

№ п/п	Раздел дисциплины	Семе-стр	Виды учебной работы (в часах)					Оценочные средства для проведения текущей и промежу-точной аттестации
			Лекция	Практические занятия	Лабора-торные	КСР	СРС	
1	2	3	4	5	6	7	8	9
	области защиты информации							
	Итого по семестру	**8**	**18**	**18**	**36**	**54**	**63**	**Экзамен**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Теоретические основы применения аудита информационной безопасности объектов (информационных технологий и систем обеспечения информационной безопасности)	2	Общие положения теории информационной безопасности (повторение и обобщение имеющихся знаний). Понятие аудита информационной безопасности	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
2.		4	Анализ и управление рисками информационной безопасности	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
3.		4	Нормативная база аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
4.	Методика проведения аудита информационной безопасности информационных технологий и систем обеспечения информационной безопасности. Лицензирование и сертификация деятельности в области защиты информации	4	Методика проведения аудита информационной безопасности исполнительных органов государственной власти и органов местного самоуправления субъектов Российской Федерации	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
5.		4	Лицензирование и сертификация деятельности в области защиты информации	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
	ВСЕГО	**18**		

6. Содержание практических/семинарских занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Теоретические основы применения аудита информационной безопасности объектов (информационных технологий и систем обеспечения информационной безопасности)	6	Формализация иерархии событий и факторов, повлиявших на становление аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ) органов исполнительной	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
			власти	
2.		4	Формирование модели аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ) на основании анализа исходных данных	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
3.		4	Организация работы ИТ-отдела в организации	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
4.		4	Организация управления аппаратными и программными ресурсами в организации	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
	ВСЕГО	**18**		

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Методика проведения аудита информационной безопасности информационных технологий и систем обеспечения информационной безопасности. Лицензирование и сертификация деятельности в области защиты информации	6	Сравнительный анализ методик проведения аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ)	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
2.		8	Проведение сравнительной характеристики систем управления конфигурацией ИТ-инфраструктуры	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
3.		8	Систематизация угроз информации, информационным ресурсам и услугам, информационной безопасности органов исполнительной власти	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
4.		8	Тестирование автоматизированных решений аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ)	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
5.		6	Проведение сравнительного анализа программ сертификации ISACA	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
	ВСЕГО	**36**		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Формализация иерархии событий и факторов, повлиявших на становление аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ) органов исполнительной власти	7	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
2.	Формирование модели аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ) на основании анализа исходных данных	7	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
3.	Организация работы ИТ-отдела в организации	7	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
4.	Организация управления аппаратными и программными ресурсами в организации	7	написание реферата, подготовка к практическому занятию, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
5.	Сравнительный анализ методик проведения аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ)	7	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
6.	Проведение сравнительной характеристики систем управления конфигурацией ИТ-инфраструктуры	7	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
7.	Систематизация угроз информации, информационным ресурсам и услугам, информационной безопасности органов исполнительной власти	7	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
8.	Тестирование автоматизированных решений аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ)	7	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
9.	Проведение сравнительного анализа программ сертификации ISACA	7	написание реферата, подготовка к лабораторной работе, подготовка к экзамену	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
	ВСЕГО	**63**		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции

1	2	3	5	6
1.	Формализация иерархии событий и факторов, повлиявших на становление аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ) органов исполнительной власти	6	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
2.	Формирование модели аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ) на основании анализа исходных данных	6	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
3.	Организация работы ИТ-отдела в организации	6	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
4.	Организация управления аппаратными и программными ресурсами в организации	6	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
5.	Сравнительный анализ методик проведения аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ)	6	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
6.	Проведение сравнительной характеристики систем управления конфигурацией ИТ-инфраструктуры	6	прием экзамена, проверка знаний на практическом занятии, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
7.	Систематизация угроз информации, информационным ресурсам и услугам, информационной безопасности органов исполнительной власти	6	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
8.	Тестирование автоматизированных решений аудита информационных технологий (ИТ) и систем обеспечения информационной безопасности (СОИБ)	6	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
9.	Проведение сравнительного анализа программ сертификации ISACA	6	прием лабораторной работы, прием экзамена, проверка реферата	ОПК-5.2.1 ОПК-5.2.2 ОПК-5.2.3 ОПК-5.4.1 ОПК-5.4.2 ОПК-5.4.3
	ВСЕГО	**54**		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Аудит информационной безопасности объектов инфокоммуникаций» используется рейтинговая система. Максимальное и минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО КНИТУ.

Рейтинговая оценка формируется на основании текущего и промежуточного контроля. За контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

Оценочные средства	Кол-во	Мин.баллов	Макс.баллов
8-й семестр			
Практические занятия	4	16	20
Лабораторная работа	5	15	30
Реферат	1	5	10
Экзамен	1	24	40
Итого		**60**	**100**

10. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Оценочные средства для проведения текущего контроля успеваемости, промежуточной аттестации и итоговой аттестации разрабатываются согласно положению о Фондах оценочных средств, рассматриваются как составная часть рабочей программы и оформляются отдельным документом.

11. Информационно-методическое обеспечение дисциплины

11.1. Основная литература

При изучении дисциплины «Аудит информационной безопасности объектов инфокоммуникаций» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
В. И. Аверченков, Аудит информационной безопасности [Электронный ресурс] Учебное пособие для вузов: Брянск : Брянский государственный технический университет, 2012	http://www.iprbookshop.ru/6991.html Режим доступа: по подписке КНИТУ
В.Ф. Шаньгин, Комплексная защита информации в корпоративных системах [Прочее] Учебное пособие: Москва : Издательский Дом "ФОРУМ", 2020	http://znanium.com/go.php?id=1093695 Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
Л.Х. Сафиуллина, А.Р. Касимова, Я.С. Рябов [и др.], Информационная безопасность. Практические аспекты [Прочее] учеб. пособие для студ. вузов спец. "Информ. безопасность": СПб. : ИЦ "Интермедия", 2021	5 экз. УНИЦ ФГБОУ ВО «КНИТУ»
Г. А. Дронова, Аттестация и аудит информационной безопасности [Прочее] учебно-методическое пособие: Новосибирск : Новосибирский государственный технический университет, 2016	http://biblioclub.ru/index.php?page=book&id=575351 Режим доступа: по подписке КНИТУ
Мельников В.П., под ред., Куприянов А.И., Васильева Т.Ю., Информационная безопасность [Прочее] Учебник: Москва : КноРус, 2020	https://www.book.ru/book/932908 Режим доступа: по подписке КНИТУ

11.3. Электронные источники информации

При изучении дисциплины «Аудит информационной безопасности объектов инфокоммуникаций» предусмотрено использование электронных источников информации:

1. Электронный каталог УНИЦ КНИТУ: Режим доступа: http://ruslan.kstu.ru/
2. ЭБС «Лань»:Режим доступа: https://e.lanbook.com
3. Образовательная платформа «Юрайт»: Режим доступа: https://urait.ru/
4. ЭБС «Znanium.com»: Режим доступа: http://znanium.com/
5. ЭБС Университетская библиотека онлайн: Режим доступа: http://biblioclub.ru/
6. ЭБС IPR SMART: Режим доступа: http://www.iprbookshop.ru/
7. ЭБС BOOK.ru : Режим доступа: https://www.book.ru/
8. Научная электронная библиотека https://elibrary.ru/

УНИЦ
Согласовано

11.4. Профессиональные базы данных и информационные справочные системы

Базы данных
Wiley Online Library: https://onlinelibrary.wiley.com/
Springer Nature: https://link.springer.com/
zbMath : https://zbmath.org/

Информационные справочные системы
Справочно-правовая система «ГАРАНТ» Доступ свободный: www.garant.ru
Справочно-правовая система «КонсультантПлюс» Доступ свободный: www.consultant.ru

12. Материально-техническое обеспечение дисциплины

Лицензированное программное обеспечение и свободно распространяемое программное обеспечение, в том числе отечественного производства, используемое в учебном процессе при освоении дисциплины «Аудит информационной безопасности объектов инфокоммуникаций»:

Офисные и деловые программы: ABBYY FineReader 9.0 проф;
Офисные и деловые программы: MS Office 2007 Russian;
Офисные и деловые программы: MS Office 2007 Professional Russian;
Офисные и деловые программы: MS Office 2010-2016 Standard
Архиватор 7 Zip
Блокнот Notepad
Яндекс Браузер

Офисные и деловые программы: 1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях
Офисные и деловые программы: Константа: Управление процессами.

Дополнительное ПО доступное по бесплатной подписке от Microsoft

Офисные и деловые программы: Microsoft Office 365 Версия для студентов
Офисные и деловые программы: Microsoft Office 365 Версия для преподавателей
ПО для коллективной работы Microsoft Teams

Moodle 3.10

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения:
1. Ноутбук на базе процессора AMD Dual-Core E-350
2. Проектор мультимедийный EB-W10, экран для проектора.
3. Экран проекционный настенный.

Помещения для самостоятельной работы оснащены компьютерной техникой:
компьютер преподавателя
11 компьютеров студента тип AMD A4-6300
кондиционер SystemAir Sysplit Wall Smart
Проектор Acer H5360BD с доской интерактивной, экран
с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ..Допускается замена оборудования его виртуальными аналогами.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Аудит информационной безопасности объектов инфокоммуникаций» составляет 9 ч.

В процессе освоения дисциплины «Аудит информационной безопасности объектов инфокоммуникаций» используются следующие образовательные технологии:

• творческие задания;
• работа в малых группах;
• дискуссия;
• обучающие игры (ролевые игры, имитации, деловые игры и образовательные игры);
• изучение и закрепление нового материала на интерактивной лекции (лекция-беседа, лекция – дискуссия, лекция с разбором конкретных ситуаций, лекция с заранее запланированными ошибками, лекция- пресс-конференция, мини-лекция).