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 **«ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»**

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; 7, 8

Вид нагрузки	Часы	Зачётные единицы
Лекция	27	0,75
Лабораторная работа	45	1,25
Контроль самостоятельной работы	81	2,25
Самостоятельная работа	108	3
Форма аттестации: Зачет (7 сем), Курсовая работа (8 сем), Экзамен (8 сем)	27	0,75
Всего	288	8

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 «Основы управления информационной безопасностью» являются:

- сформировать у студентов навыки реализации мероприятий по управлению информационной безопасностью;
- дать студентам представление об устранении рисков информационной безопасности:
- обучить студентов принципам управления информационной безопасностью.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Основы управления информационной безопасностью» 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 «Основы управления информационной безопасностью» обучающийся по направлению подготовки 10.03.01 «Информационная безопасность» должен освоить материал предшествующих дисциплин:

1. Защита и обработка конфиденциальных документов
2. История и современная система защиты информации
3. Основы информационной безопасности
4. Теория информации

Дисциплина «Основы управления информационной безопасностью» является предшествующей и необходима для успешного освоения последующих дисциплин:

1. Защита информации от утечки по техническим каналам
2. Проектирование защищенных телекоммуникационных систем
3. Специализированные вычислительные устройства защиты информации

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;

ОПК-10.1. Знает современные принципы рационального выбора средств защиты в зависимости от вида объекта защиты, системный подход к выполнению и организации проектирования средств защиты, нормативные и распорядительные документы, регламентирующие деятельность по обеспечению защищенности объектов информатизации в условиях существовании угроз предприятия, подразделений, должностные инструкции

ОПК-10.2. Умеет применять стандарты по оценке защищенности автоматизированных систем при анализе и проектировании систем защиты информации в автоматизированныз системах, выполнять обследование объектов обеспечения защищенности информации в условиях существовании угроз, анализ предметной области в соответствии с поставленными задачами

ОПК-10.3. Владеет современными методами оценки и исследования информационной безопасности различных объектов

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-6.1. Знает правила лицензирования и сертификации в области защиты информации,основы правового регулирования взаимоотношений администрации и персонала в области защиты информации

ОПК-6.2. Умеет отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства; применять действующую законодательную базу в области защиты информации

ОПК-6.3. Владеет современными методами оценки и исследования информационной безопасности различных

объектов,алгоритмом процессом работы с конфиденциальным электронным документом

В результате освоения дисциплины обучающийся должен

Знать:

нормативные правовые акты, нормативные и методические документы организации защиты информации

задачи защиты информации ограниченного доступа

современные принципы рационального выбора средств защиты в зависимости от вида объекта защиты,

системный подход к выполнению и организации проектирования средств защиты

Уметь:

организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности,

выполнять обследование объектов обеспечения защищенности информации в условиях существовании угроз

применять необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства

Владеть:

методами оценки и исследования информационной безопасности различных объектов,

навыками алгоритмизации процессов работы с конфиденциальным электронным документом

современными методами оценки и исследования информационной безопасности различных объектов

4. Структура и содержание дисциплины

Общая трудоёмкость дисциплины составляет 8 зачетных единиц, 288 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.	Информационная безопасность как объект управления	7	5		4	9	18	Лабораторная работа; Реферат
2.	Система управления информационной безопасностью	7	4		5	9	18	
	Итого по семестру	**7**	**9**		**9**	**18**	**36**	**Зачет**
1.	Организация процесса управления информационной безопасностью	8	10		16	20	18	Лабораторная работа

№ 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
2.	Оценка деятельности по управлению информационной безопасностью	8	8		20	20	18	Лабораторная работа; Экзамен
3.	Курсовая работа	8				23	36	Курсовая работа
	Итого по семестру	**8**	**18**		**36**	**63**	**72**	**Курсовая работа, Экзамен**

5. Содержание лекционных занятий по темам

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
1.	Информационная безопасность как объект управления	2	Информационная безопасность в системе национальной безопасности России	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
2.		2	Основные определения и критерии классификации угроз информационной безопасности	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
3.		1	Современные проблемы обеспечения информационной безопасности и пути их решения	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
4.	Система управления информационной безопасностью	1	Подходы к управлению информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
5.		1	Стратегии построения и внедрения системы управления информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
6.		1	Процессы управления информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
7.		1	Стандартизация процессов управления информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2

№ п/п	Раздел дисциплины	Часы	Тема лекционного занятия	Индикаторы достижения компетенции
1	2	3	4	5
				ОПК-6.3
8.	Организация процесса управления информационной безопасностью	2	Модели организационного управления информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
9.		2	Организационная инфраструктура управления информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
10.		4	Организация службы информационной безопасности	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
11.		2	Кадровое обеспечение управления информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
12.	Оценка деятельности по управлению информационной безопасностью	2	Оценка эффективности и результативности деятельности по управлению информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
13.		2	Измерение информационной безопасности	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
14.		4	Оценка зрелости процессов в системе управления информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
	ВСЕГО	**27**		

6. Содержание практических/семинарских занятий

Проведение практических/семинарских занятий не предусмотрено учебным планом

7. Содержание лабораторных занятий

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
1.	Информационная безопасность как объект управления	2	Принципы, задачи и функции обеспечения информационной безопасности	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2

№ п/п	Раздел дисциплины	Часы	Тема занятия	Индикаторы достижения компетенции
1	2	3	4	6
				ОПК-6.3
2.		2	Характеристика угроз информационной безопасности	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
3.	Система управления информационной безопасностью	2	Модели систем и процессов защиты информации	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
4.		3	Построение и внедрение системы управления информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
5.	Организация процесса управления информационной безопасностью	8	Организационные каналы утечки информации	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
6.		8	Организационные мероприятия по управлению информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
7.	Оценка деятельности по управлению информационной безопасностью	10	Эффективность и результативность управления информационной безопасности	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
8.		10	Измерения, связанные с информационной безопасностью	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
	ВСЕГО	**45**		

8. Самостоятельная работа

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
1.	Принципы, задачи и функции обеспечения информационной безопасности	10	написание реферата, подготовка к лабораторной работе	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
2.	Характеристика угроз информационной безопасности	8	написание реферата, подготовка к лабораторной работе	ОПК-10.1 ОПК-10.2

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма СРС	Индикаторы достижения компетенции
1	2	3	5	6
				ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
3.	Модели систем и процессов защиты информации	8	написание реферата, подготовка к лабораторной работе	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
4.	Построение и внедрение системы управления информационной безопасностью	10	написание реферата, подготовка к лабораторной работе	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
5.	Организационные каналы утечки информации	9	подготовка к лабораторной работе	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
6.	Организационные мероприятия по управлению информационной безопасностью	9	подготовка к лабораторной работе	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
7.	Эффективность и результативность управления информационной безопасности	9	подготовка к лабораторной работе	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
8.	Измерения, связанные с информационной безопасностью	9	подготовка к лабораторной работе, подготовка к экзамену	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
9.	Курсовая работа	36	выполнение курсовой работы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
	ВСЕГО	**108**		

8.1 Контроль самостоятельной работы

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
1.	Характеристика угроз информационной безопасности	5	прием лабораторной работы, проверка реферата	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
2.	Принципы, задачи и функции обеспечения информационной безопасности	4	прием лабораторной работы, проверка реферата	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1

№ п/п	Темы, выносимые на самостоятельную работу	Часы	Форма КСР	Индикаторы достижения компетенции
1	2	3	5	6
				ОПК-6.2 ОПК-6.3
3.	Модели систем и процессов защиты информации	4	написание реферата, прием лабораторной работы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
4.	Построение и внедрение системы управления информационной безопасностью	5	прием лабораторной работы, проверка реферата	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
5.	Организационные каналы утечки информации	10	прием лабораторной работы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
6.	Организационные мероприятия по управлению информационной безопасностью	10	прием лабораторной работы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
7.	Эффективность и результативность управления информационной безопасности	10	прием лабораторной работы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
8.	Измерения, связанные с информационной безопасностью	10	прием лабораторной работы, прием экзамена	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
9.	Курсовая работа	23	проверка курсовой работы	ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-6.1 ОПК-6.2 ОПК-6.3
	ВСЕГО	**81**		

9. Использование рейтинговой системы оценки знаний

При оценке результатов деятельности обучающихся в рамках дисциплины «Основы управления информационной безопасностью» 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
7-й семестр			
Лабораторная работа	4	52	80
Реферат	1	8	20

Итого		**60**	**100**
8-й семестр			
Лабораторная работа	4	36	60
Экзамен	1	24	40
Итого		**60**	**100**
8-й семестр			
Курсовая работа	1	60	100
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 «Основы управления информационной безопасностью» в качестве основных источников информации рекомендуется использовать следующую литературу:

Основные источники информации	Количество экземпляров
Э. Мэйволд,, Безопасность сетей [Прочее] учебное пособие: Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021	http://www.iprbookshop.ru/101992.html Режим доступа: по подписке КНИТУ
Е. С. Кубашева, Е. Н. Чекулаева, Управление информационной безопасностью [Прочее] учебное пособие: Йошкар-Ола : Поволжский государственный технологический университет, 2020	https://biblioclub.ru/index.php?page=book&id=612591 Режим доступа: по подписке КНИТУ
О. А. Чернова, Управление промышленным предприятием в условиях информационной экономики [Прочее] учебное пособие: Ростов-на-Дону|Таганрог : Южный федеральный университет, 2020	http://biblioclub.ru/index.php?page=book&id=598550 Режим доступа: по подписке КНИТУ

11.2. Дополнительная литература

В качестве дополнительных источников информации рекомендуется использовать следующую литературу:

Дополнительные источники информации	Количество экземпляров
А. В. Никулин,, В. В. Артюшенко,, Компьютерные сети и телекоммуникации [Прочее] учебно-методическое пособие по русскому языку как иностранному: Новосибирск : Новосибирский государственный технический университет, 2020	http://www.iprbookshop.ru/99345.html Режим доступа: по подписке КНИТУ
Ибе Оливер, Компьютерные сети и службы удаленного доступа [Электронный ресурс] : Саратов : Профобразование, 2019	http://www.iprbookshop.ru/87999.html Режим доступа: по подписке КНИТУ
Г. А. Дронова, Управление информационной безопасностью [Прочее] учебно-методическое пособие: Новосибирск : Новосибирский государственный технический университет, 2016	http://biblioclub.ru/index.php?page=book&id=575356 Режим доступа: по подписке КНИТУ
М. Н. Жукова, В.Г. Жуков, Управление информационной безопасностью. Ч. 2.	http://znanium.com/go.php?id=463061 Режим доступа: по подписке КНИТУ

Управление инцидентами информационной безопасности [Прочее] : Красноярск : Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева, 2012	
А. . Сатунина, Л. . Сысоева, Управление проектом корпоративной информационной системы предприятия [Учебник] учеб. пособие для студ. вузов, обуч. по спец. "Прикладная информатика (по областям)": М. : Финансы и статистика : ИНФРА-М, 2009	1 экз. УНИЦ ФГБОУ ВО «КНИТУ»

11.3. Электронные источники информации

При изучении дисциплины «Основы управления информационной безопасностью» 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 «Основы управления информационной безопасностью»:

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

Учебные аудитории для проведения учебных занятий оснащены оборудованием и техническими средствами обучения:

Аудитория 351-А;
1. Виртуальные машины VirtualBOX (GNU GENERAL PUBLIC LICENSE)
2. Симулятор сетей GNS3 (GNU GENERAL PUBLIC LICENSE)
3. Операционная система Linux (Fedora, Ubuntu). (GNU GENERAL PUBLIC LICENSE)
4. RADIUS сервер (GNU GENERAL PUBLIC LICENSE)
5. Sendmail - SMTP сервер (Sendmail License)
6. POP3 сервер (BSD License)
7. IMAP4 сервер (BSD License)
8. NTP сервер (BSD License)
9. Межсетевой экран iptables (GNU GENERAL PUBLIC LICENSE)
10. Межсетевой экран Firewalld (GNU GENERAL PUBLIC LICENSE)
11. Сканер сетевой безопасности nmap (GNU GENERAL PUBLIC LICENSE)
12. Система обнаружения атак snort (GNU GENERAL PUBLIC LICENSE)
13. Система синхронизации данных rsync
14. компьютер/ноутбук
техническими средствами обучения:
1. Типовой комплект учебного оборудования «Глобальные компьютерные сети» ,
2. Типовой комплект учебного оборудования «Корпоративные компьютерные сети» .
Помещения для самостоятельной работы оснащены компьютерной техникой:
Аудитория Г-409, компьютер/ноутбук с возможностью подключения к сети «Интернет» и обеспечены доступом в электронную информационную среду КНИТУ.

13. Образовательные технологии

Количество часов занятий, проводимых в интерактивных формах в учебном процессе по дисциплине «Основы управления информационной безопасностью» составляет 18 ч.

В процессе освоения дисциплины «Основы управления информационной безопасностью» 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);