МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

«МЕТОДЫ АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ»

Уровень подготовки: высшее образование – магистратура

Направление подготовки
09.04.01 Информатика и вычислительная техника
(код и наименование направления подготовки)

Направленность подготовки
Безопасность и защита информации
(наименование программы подготовки)

Квалификация (степень) выпускника
Магистр

Форма обучения
очная

Уфа 2017

Место дисциплины в структуре образовательной программы

Дисциплина «Методы анализа информационных рисков» является дисциплиной *вариативной* части ОПОП по направлению подготовки 09.04.01 Информатика и вычислительная техника, направленность: Безопасность и защита информации. Дисциплина является обязательной частью программы обучения магистрантов.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.04.01 Информатика и вычислительная техника (уровень магистратуры)», утвержденного приказом Министерства образования и науки Российской Федерации от "30" октября 2014 г. № 1420. Является неотъемлемой частью основной образовательной профессиональной программы (ОПОП).

Целью освоения дисциплины является формирование у будущих магистров теоретических знаний и практических навыков для решения научно-исследовательских и прикладных задач, связанных с применением методов анализа и оценки рисков нарушения информационной безопасности, а также с методами снижения уровня рисков и повышения уровня защищенности объекта защиты.

Задачи:

- Сформировать знания по теоретическим и методологическим положениям теории информационных рисков, терминологии дисциплины;
- Сформировать представление о современных методах оценки риска нарушения информационной безопасности объектов информатизации;
- Изучить положения теории рисков и основные этапы проведения анализа рисков объектов информатизации;
- Изучить отечественную и зарубежную нормативную правовую базу по оценке рисков нарушения информационной безопасности;
- Изучить основные научные подходы, методы и алгоритмы оценивания информационных рисков, способы снижения риска на объекте информатизации и повышения уровня защищенности объекта;
- Приобрести практический опыт использования программ и программных комплексов, реализующих методы анализа информационных рисков;
- Приобрести практический навык составления отчетов по проведенному анализу информационных рисков.

Дисциплина является самостоятельным элементом в системе подготовки магистров информатики и вычислительной техники. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- Управление информационной безопасностью;
- Проектирование защищенных компьютерных систем.

В дисциплине «*Методы анализа информационных рисков*» определяются теоретические основы и практические навыки, при освоении которых магистрант способен приступить к прохождению научно-исследовательской практики и выполнять научные исследования в соответствующей предметной области.

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции*	Название дисциплины (модуля), практики, научных исследований, сформировавших данную компетенцию
1	способность к профессиональной эксплуатации современного оборудования и приборов	ОК-8	Базовый уровень, первый этап	Вычислительные системы

2	владение методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях	ОПК-5	Базовый уровень, первый этап	Вычислительные системы
3	способность формировать технические задания и участвовать в разработке аппаратных и (или) программных средств вычислительной техники;	ПК-11	Базовый уровень, первый этап	Системный анализ
4	способность выбирать методы и разрабатывать алгоритмы решения задач управления и проектирования объектов автоматизации	ПК-12	Базовый уровень, первый этап	Системный анализ, Методы оптимизации

Исходящие компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований для которых данная компетенция является входной
1	способность к профессиональной эксплуатации современного оборудования и приборов	ОК-8	Базовый уровень, второй этап	Научно-исследовательская работа
2	владение методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях	ОПК-5	Базовый уровень, второй этап	Интегрированные системы безопасности объектов информатизации, Интеллектуальные системы защиты информации, Информационно-аналитические системы безопасности
3	способность формировать технические задания и участвовать в разработке аппаратных и (или) программных средств вычислительной техники	ПК-11	Базовый уровень, второй этап	Научно-исследовательская практика, Государственная итоговая аттестация
4	способность выбирать методы и разрабатывать алгоритмы решения задач управления и проектирования объектов автоматизации	ПК-12	Базовый уровень, второй этап	Интеллектуальные системы, Интеллектуальные системы защиты информации, Информационно-аналитические системы безопасности

2. Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	способность к профессиональной эксплуатации современного оборудования и приборов	ОК-8	- основные программные продукты и комплексы, в которых реализованы современные методы анализа риска нарушения информационной безопасности; -нормативную правовую базу, которую можно применить для качественной оценки информационного риска	-проводить количественный анализ рисков нарушения информационной безопасности предприятия на основе современных программных продуктов и комплексов; -грамотно составить сводный отчет на основе рассчитанных программными продуктами значений риска нарушения информационной безопасности организации.	- современными программными продуктами и комплексами, в которых реализованы современные методы анализа риска нарушения информационной безопасности.
	владение методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях	ОПК-5	- основные угрозы информационной безопасности предприятия, их источники и последствия; -основные способы и методы повышения уровня защищенности предприятия; - общие принципы сбора и обработки информации на предприятии, моделирования бизнес-процессов предприятия.	-выявлять источники угроз конфиденциальности, целостности и доступности информации; -выявлять внешние и внутренние угрозы информационной безопасности предприятия; -качественно оценивать риск нарушения информационной безопасности на основе экспертных оценок; -работать с современной нормативной правовой базой РФ и нормативными документами предприятия, включая политику безопасности организации; -работать с автоматизированными ба-	-методами и средствами сбора, хранения и обработки информации с использованием современных компьютерных технологий, направленных на анализ рисков нарушения информационной безопасности.

				зами данных уязвимостей.	
	способность формировать технические задания и участвовать в разработке аппаратных и (или) программных средств вычислительной техники;	ПК-11	-основные требования по повышению уровня защищенности предприятия; -основные принципы выбора наилучшего состава средств защиты информации на предприятии; -основные понятия архитектуры системы информационной безопасности предприятия.	-составлять технические задания, направленные на повышение уровня защищенности предприятия и снижение риска нарушения информационной безопасности; -разрабатывать программные средства, реализующие методы анализа риска нарушения информационной безопасности, составления перечня наилучших вариантов выбора программных/аппаратных и программно-аппаратных средств защиты информации.	-способами формирования технического задания для повышения уровня защищенности и снижения информационных рисков на предприятии; -способами разработки программных средств, реализующих методы анализа риска нарушения информационной безопасности, составления перечня наилучших вариантов выбора программных/аппаратных и программно-аппаратных средств защиты информации.
	способность выбирать методы и разрабатывать алгоритмы решения задач управления и проектирования объектов автоматизации	ПК-12	-существующие методы и алгоритмы качественного и количественного анализа информационных рисков; -отечественную и зарубежную нормативную правовую базу в области рисков нарушения информационной безопасности и программные продукты на их основе.	-составлять перечень критичных активов предприятия; -составлять перечень и моделировать бизнес-процессы предприятия; -находить уязвимости в программных/аппаратных и программно-аппаратных средствах и комплексах на предприятии; -выбирать варианты реагирования на опасные события.	-современными методами и алгоритмами качественного и количественного анализа информационных рисков.

3. Содержание и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.
	1 семестр
Лекции (Л)	16
Практические занятия (ПЗ)	30
Лабораторные работы (ЛР)	8
КСР	5
Курсовой проект/работа (КР)	не предусмотрено планом
Расчетно - графическая работа (РГР)	не предусмотрено планом
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)	112
Подготовка и сдача экзамена	не предусмотрено планом
Подготовка и сдача зачета	9
Вид итогового контроля (зачет, экзамен)	зачет

Содержание разделов и формы текущего контроля

№	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая студентам*	Виды интерактивных образовательных технологий**
		Аудиторная работа				СРС	Всего		
		Л	ПЗ	ЛР	КСР				
1	**Основные понятия в области анализа управления информационными рисками. Нормативо-правовая база анализа информационных рисков.** Понятие риска. Цели и задачи анализа рисков нарушения информационной безопасности (ИБ). Этапы процесса управления рисками. Основные положения стандарта ГОСТ Р 51897-2011 «Менеджмент риска. Термины и определения». Эталонная модель рисков. Основные положения национальных стандартов ГОСТ Р ИСО/МЭК 2700xx в области анализа и управления информационными рисками. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (СТО БР ИББС-1.0-2014). Нормативно-методические документы ФСТЭК.	4	2			30	36	Р.6.1, №1, гл.1 Р.6.1, №3, гл.1 Р.6.2, №2, гл.1 Р.6.2, №4, гл.1,2 Р.6.2, №5, гл.2,3 Р.6.2, №№7-12	Лекция классическая, лекция проблемная, при проведении практических занятий: – проблемное обучение; – обучение на основе опыта.
2	**Технологии анализа информационных рисков.** Методология анализа информационных рисков OCTAVE. Методики качественного анализа рисков нарушения ИБ (CRAMM, CORAS, COBRA, FRAP, NIST). Методы количественного анализа рисков нарушения ИБ (Risk Watch, MSAT, Гриф 2006, Кондор 2006). Идентификация информационных активов, угроз и уязвимостей. Оценка потенциального ущерба от воздействия угроз, меры по снижению информационных рисков. Разработка итоговых отчетов	6	10	8		40	64	Р.6.1, №1, гл.5 Р.6.1, №2, гл.1 Р.6.2, №1, гл.1 Р.6.2, №4, гл.4,5 Р.6.2, №5, гл.4,5 Р.6.2, №6, гл.1 Р.6.2, №№7-11	Лекция классическая, лекция проблемная, при проведении практических занятий: – проблемное обучение; – обучение на основе опыта.

	по анализу и управлению рисками.								
3	**Методы и модели аналитической оценки информационных рисков.** Модель СЗИ с полным перекрытием. Оценка рисков с помощью нечетких когнитивных карт. Системы нечеткого логического вывода. Оценка рисков с помощью нейронных сетей. Нечеткие нейронные сети (ANFIS). Марковские модели. Инструментальные средства (программные пакеты) для оценки информационных рисков.	4	18		3	30	55	Р.6.1, №1, гл.4,5 Р.6.1, №3, гл.3 Р.6.2, №1, гл.2,3 Р.6.2, №2, гл.2 Р.6.2, №3, гл.5 Р.6.2, №5, гл.6 Р.6.2, №6, гл.4	Лекция классическая, лекция проблемная, при проведении практических занятий: – проблемное обучение; – обучение на основе опыта.
4	**Аудит информационной безопасности.** Понятие аудита, виды аудита ИБ. Экспертные системы. Интеллектуальные системы поддержки принятия решений (ИСППР) при проведении аудита ИБ. Пример построения ИСППР по оценке риска и уровня защищенности ИС ПДн. SIEM-системы, архитектура, функции и решаемые задачи по оценке рисков.	2			2	12	16	Р.6.1, №2, гл.3 Р.6.2, №2, гл.4 Р.6.2, №4, гл.5 Р.6.2, №6, гл.5 Р.6.2, №№7-12	Лекция классическая, лекция проблемная, при проведении практических занятий: – проблемное обучение; – обучение на основе опыта.

**Указывается номер источника из соответствующего раздела рабочей программы, раздел (например, Р 6.1 №1, гл.3)*

***Указываются образовательные технологии, используемые при реализации различных видов работы.*

Занятия, проводимые в интерактивной форме, составляют 10% от общего количества аудиторных часов по дисциплине "Методы анализа информационных рисков".

Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
2	2	Изучение функциональных возможностей программного комплекса оценки защищенности организаций MSAT	4
1	2	Применение программного комплекса MSAT для оценки уровня рисков информационной безопасности предприятия	4

Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	**1**	Анализ критичных активов предприятия, разработка модели бизнес-процессов предприятия, выявление основных источников угроз на предприятии	2
2,3	**2**	Оценка информационных рисков на основе анализа по информационным потокам с помощью программного продукта ГРИФ 2006	4
4,5	**2**	Оценка информационных рисков на основе анализа требований стандарта ГОСТ 27002 с помощью программного продукта Кондор 2006	4
6	**2**	Работа с международной базой уязвимости (NVD), определение уровня уязвимости компонентов локальной вычислительной сети предприятия	2
7,8	**3**	Расчет рисков ИБ с помощью системы нечеткого логического вывода	4
9,10	**3**	Расчет рисков нарушения информационной безопасности предприятия с помощью нечетких когнитивных карт	4
11-13	**3**	Расчет рисков нарушения ИБ с помощью нейронных сетей	6
14,15	**3**	Расчет рисков ИБ предприятия с помощью Марковских моделей	4

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1 Основная литература

1. Гузаиров М.Б. Управление защитой информации на основе интеллектуальных технологий [учеб. пособие для вузов] / М.Б. Гузаиров, И.В. Машкина. – М.: Машиностроение, 2013. – 241 с.

2. Юсупова Н.И. Интеллектуальная информационная поддержка принятия решений при анализе рисков чрезвычайных ситуаций и управлении ими / Н.И. Юсупова, К.Р. Еникеева. – Уфа: УГАТУ, 2014. – 206 с.

3. Михайлов Ю.Б. Научно-методические основы обеспечения безопасности защищаемых объектов. – М.: Горячая линия – Телеком, 2015. – 322 с.

6.2 Дополнительная литература

1. Машкина И.В. Анализ риска объекта информатизации [учеб. пособие] / И.В. Машкина, Е.С. Степанова, Т.О. Вишнякова. – Уфа: УГАТУ, 2011. – 112 с.

2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [учеб. пособие]. – М.: Форум: Инфра-М., 2013. – 415 с.

3. Васильев В.И. Информационные системы защиты информации [учеб. пособие для вузов]. – 2-е изд. – М.: Машиностроение, 2012. – 152 с.

4. Петренко С.А. Управление информационными рисками: Экономически оправданная безопасность. – М.: Компания АйТи: ДМК Пресс, 2005. – 384 с.

5. Астахов А.М. Искусство управления информационными рисками. – М.: ДМК Пресс, 2010. – 312 с. [Электронный ресурс]: URL: https://eknigi.org/nauka_i_ucheba/.../html (дата обращения: 02.09.2015).

6. Варфоломеев А.А. Управление информационными рисками [учеб. пособие] – М.: Изд-во РУДН, 2008. – 158 с. [Электронный ресурс]: URL: web-local.rudn.ru/web-local/uem/iop_pdf/52-Varfolomeev.pdf (дата обращения: 02.09.2015).

7. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», введ. 01.02.2008. – М: Стандартинформ, 2008. – 31 с.

8. ГОСТ Р ИСО/МЭК 27002-2012 «Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», введ. 01.01.2014. – М: Стандартинформ, 2014. – 210 с.

9. ГОСТ Р ИСО/МЭК 27003-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности», введ. 01.12.2013. – М: Стандартинформ, 2013. – 257 с.

10. ГОСТ Р ИСО/МЭК 27004-2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения», введ. 01.01.2013. – М: Стандартинформ, 2012. – 62 с.

11. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», введ. 01.12.2011. – М: Стандартинформ, 2011. – 51 с.

12. ГОСТ Р ИСО/МЭК 27006-2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности», введ. 01.10.2009. – М: Стандартинформ, 2009. – 39 с.

13. ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности», введ. 11.06.2014. – М: Стандартинформ, 2014. – 50 с.

6.3. Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки http://library.ugatu.ac.ru/ в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

Обучающимся обеспечен доступом к м электронным ресурсам и информационным справочным системам, перечисленным в таблице

№	Наименование ресурса	Объем фонда электронных ресурсов	Доступ	Реквизиты договоров с правообладателями
1.	Электронная библиотека диссертаций РГБ http://dvs.rsl.ru	885 898 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор №2255/0208-15 от 23.12.2015
2.	База данных Proquest Dissertations and Theses Global http://search.proquest.com/	более 3,5 млн. диссертаций и дипломных работ	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и Государственной публичной научно-технической библиотекой России (далее ГПНТБ России) Сублиц. договор №ProQuest/151 52/0208-16 от 02.06.2016
3.	СПС «КонсультантПлюс»	2007691 экз.	По сети УГАТУ	Договор 3К-2318/0106-15 от 30.12.2015
4.	СПС «Гарант»	6139026 экз.	Доступ с компьютеров читальных залов библиотеки, подключенных к ресурсу	Договор 15\0208-16 от 15.03.2016
5.	ИПС «Технорма/Документ»	36939 экз.	Локальная установка: библиотека УГАТУ-5 мест; кафедра стандартизации и метрологии-1место; кафедра начертательной геометрии и черчения-1 место	Договор № АОСС/914-15 № 989/0208-15 от 08.06.2015.
6.	Научная электронная библиотека eLIBRARY*	9919 полнотекстовых	С любого компьютера,	ООО «НАУЧНАЯ ЭЛЕКТРОННАЯ

	http://elibrary.ru/	журналов	имеющего выход в Интернет, после регистрации в НЭБ на площадке библиотеки УГАТУ	БИБЛИОТЕКА». № 07-06/06 от 18.05.2006
7.	Патентная база данных компании Questel Orbit* http://www.orbit.com	55 млн. документов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор№Questel/151 46/0208-16 от 02.06.2016
8.	Научные полнотекстовые журналы издательства Taylor& Francis Group* http://www.tandfonline.com/	1700 наимен. журнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №T&F/151 44/0208-16 от 02.06.2016
9.	Научные полнотекстовые журналы издательства Sage Publications* http://online.sagepub.com/	790 наимен. жрнал.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Sage/151 47/0208-16 от 02.06.2016
10.	Научные полнотекстовые журналы издательства Oxford University Press* http://www.oxfordjournals.org/	255 наимен. Журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством

				образования и науки РФ и ГПНТБ России Сублиц. договор №OUP-151 43/0208-16 от 02.06.2016
11.	База данных Computers & Applied Sciences Complete компании EBSCO Publishing http://search.ebscohost.com	1000 наим. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №CASC/151 50/0208-16 от 02.06.2016
12.	Научный полнотекстовый журнал Science The American Association for the Advancement of Science http://www.sciencemag.org	1 наимен. журнала.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №Science/151 45/0208-16 от 02.06.2016
13.	Научные полнотекстовые журналы Американского института физики http://scitation.aip.org/	18 наимен. журналов	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №AIP/151 48/0208-16 от 02.06.2016
14.	Научные полнотекстовые ресурсы Optical Society of America*	9 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего	В рамках Государственного контракта от 17.02.2016 г.

	http://www.opticsinfobase.org/		выход в Интернет	№14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. договор №OSA/151 49/0208-16 от 02.06.2016
15.	База данных GreenFile компании EBSCO* http://www.greeninfoonline.com	5800 библиографич записей, частично с полными текстами	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен компанией EBSCO российским организациям-участникам консорциума НЭИКОН (в т.ч. УГАТУ - без подписания лицензионного договора)
16.	Реферативная база данных INSPEC компании EBSCO Publishing http://search.ebscohost.com	Более 11 млн. библиографич записей		В рамках Государственного контракта от 17.02.2016 г. №14.596.11.0014 между Министерством образования и науки РФ и ГПНТБ России Сублиц. Договор №INSPEC/151 51/0208-16 от 02.06.2016
17.	Архив научных полнотекстовых журналов зарубежных издательств*- http://archive.neicon.ru Annual Reviews (1936-2006) Cambridge University Press (1796-2011) цифровой архив журнала Nature (1869- 2011) Oxford University Press (1849–1995) SAGE Publications (1800-1998) цифровой архив журнала	2361 наимен. журн.	С любого компьютера по сети УГАТУ, имеющего выход в Интернет	Доступ предоставлен российским организациям-участникам консорциума НЭИКОН (в т. ч. УГАТУ - без подписания лицензионного договора)

	Science (1880 -1996) Taylor & Francis (1798-1997) Институт физики Великобритании The Institute of Physics (1874-2000)			

7. Методические указания по освоению дисциплины

Формы работы студентов: лекционные занятия, практические занятия, лабораторные работы, написание рефератов, решение кейс-задач.

Дисциплина «Методы анализа информационных рисков» разбита на модули, представляющие собой логически завершенные части курса и являющиеся теми комплексами знаний и умений, которые подлежат контролю.

Контроль освоения лекционных тем включает в себя выполнение кейс-задач.

В качестве организованной самостоятельной работы студента рекомендуется использовать написание рефератов по выбранной заранее тематике. При написании реферата студент должен в соответствии с требованиями к оформлению работ сформулировать проблему, актуальность, поставить цель и задачи исследования, сделать самостоятельный вывод о состоянии и путях решения заданной проблемы.

8 . Материально-техническое обеспечение дисциплины

Перечень лекционных аудиторий с современными средствами демонстрации – 5-301, 5-314, 5-313, 5-317.

Перечень лабораторий современного, высокотехнологичного оборудования, обеспечивающего реализацию ОПОП ВО с учетом направленности подготовки:

- 5-304 – компьютерный класс;
- 5-408 – лаборатория технических средств защиты информации.

Вычислительное и телекоммуникационное оборудование и программные средства, необходимых для реализации ОПОП ВО и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности:

- компьютерная техника:
  - Intel Core i7-4790/ASUS Z97-K DDR3 ATX SATA3/Kingston DDR-III 2x4Gb 1600MHz/Segate 1Tb SATA-III/ Kingston SSD Disk 240Gb; серверы: CPU Intel Xenon E3-1240 V3 3.4GHz/4core/1+8Mb/80W/5GT ASUS P9D-C /4L LGA1150 / PCI-E SVGA 4xGbLAN SATA ATX 4DDR-III HDD 3 Tb SATA 6Gb/s Seagate Constellation CS 3,5” 7200rpm 64 Mb Crucia <CT102472BD160B> DDR-III DIMM 2x8Gb <ST3000NC002> CL11;
- программное обеспечение:
  - Программный комплекс – операционная система Microsoft Windows (№ договора ЭФ-193/0503-14, 1800 компьютеров, на которые распространяется право пользования)
  - Программный комплекс – Microsoft Office (№ договора ЭФ-193/0503-14, 1800 компьютеров, на которые распространяется право пользования)
  - Программный комплекс – Microsoft Project Professional (№ договора ЭФ-193/0503-14, 50 компьютеров, на которые распространяется право пользования)

- Программный комплекс – операционная система Microsoft Visio Pro (№ договора ЭФ-193/0503-14, 50 компьютеров, на которые распространяется право пользования)
- Kaspersky Endpoint Security для бизнеса (лицензии 13C8-140128-132040, 500 users).
- Dr.Web® Desktop Security Suite (КЗ) +ЦУ (AH99-VCUN-TPPJ-6k3L, 415 рабочих станций).
- ESET Smart Security Business (EAV-8424791, 500 пользователей).
- Контур информационной безопасности SearchInform (UEI-2349-87, 25 пользователей).
- Secret Net (IEK-109869, 25пользователей).
- InfoWatch Traffic Monitor Enterprise (IWES-S3-DE, 25пользователей).
- Seagate Central Discovery для ОС Windows (WOS-65-GT5, 25пользователей).

При обучении инвалидов и лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, обеспечивается возможность беспрепятственного доступа в учебные помещения и пункты питания и другие, необходимые для жизнедеятельности помещения, оборудованные пандусами, лифтами и иными средствами, облегчающими процесс передвижения. Для лиц с ограниченными возможностями здоровья по зрению предусматривается возможность доступа к зданию с собакой-поводырем.

9. Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.