Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов имени Патриса Лумумбы»

Факультет искусственного интеллекта

(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование направления подготовки/специальности)

Освоение дисциплины ведется в рамках реализации основной профессиональной образовательной программы высшего образования (ОП ВО):

ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Основы управления информационной безопасностью» входит в программу бакалавриата «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» по направлению 10.03.01 «Информационная безопасность» и изучается в 6 семестре 3 курса. Дисциплину реализует Кафедра информационной безопасности . Дисциплина состоит из 1 раздела и 10 тем и направлена на изучение принципов и методов управления процессами управления информационной безопасностью в организациях. В рамках этого курса студенты знакомятся с основами стратегического и оперативного управления защитой информации, созданием и реализацией политик информационной безопасности, а также контролем и мониторингом состояния защищенности информационных систем.

Целью освоения дисциплины является формирование у студентов знаний и навыков, необходимых для эффективного управления процессами защиты информации в организациях, включая разработку и реализацию политик информационной безопасности, оценку рисков и управление ими, а также контроль и мониторинг состояния защищённости информационных систем.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Основы управления информационной безопасностью» направлено на формирование у обучающихся следующих компетенций (части компетенций):

Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)

Шифр	**Компетенция**	**Индикаторы достижения компетенции** (в рамках данной дисциплины)
УК-11	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-11.1 Анализирует действующие правовые нормы, обеспечивающие борьбу с экстремизмом, терроризмом, коррупционным поведением в различных областях жизнедеятельности, а также способы профилактики экстремизма, терроризма, коррупционного поведения и формирования нетерпимого отношения к ним; УК-11.2 Соблюдает правила общественного взаимодействия на основе соблюдения действующего законодательства и нетерпимого отношения к экстремизму, терроризму, коррупционному поведению;
ОПК-16	Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК-16.1 Знает меры по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности; ОПК-16.2 Разрабатывает, внедряет и сопровождает комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ОПК-17	Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ОПК-17.1 Знает методы и средства проведения аудита защищенности объекта информатизации в соответствии с нормативными документами;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Основы управления информационной безопасностью» относится к обязательной части блока 1 «Дисциплины (модули)» образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Основы управления информационной безопасностью».

Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины

Шифр	**Наименование компетенции**	**Предшествующие дисциплины/модули, практики***	**Последующие дисциплины/модули, практики***
УК-11	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	Исследовательская практика; Основы российской государственности; Правоведение; Ознакомительная практика;	Преддипломная практика; Технологическая практика;
ОПК-16	Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности		Комплексное обеспечение защиты информации объекта информатизации; Технологическая практика;
ОПК-17	Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами		Аудит информационной безопасности;

* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Основы управления информационной безопасностью» составляет «3» зачетные единицы.

Таблица 4.1. Виды учебной работы по периодам освоения образовательной программы высшего образования для очной формы обучения.

Вид учебной работы	**ВСЕГО,** ак.ч.		**Семестр(-ы)**
			6
Контактная работа, ак.ч.	*52*		*52*
Лекции (**ЛК**)	26		26
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	26		26
Самостоятельная работа обучающихся, ак.ч.	*29*		*29*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины	**ак.ч.**	***108***	*108*
	зач.ед.	***3***	*3*

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 1	Основы управления информационной безопасностью	1.1	Оценочные стандарты в информационной безопасности	Роль стандартов ИБ. «Оранжевая книга» как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.	ЛК, СЗ
		1.2	Стандарты управления информационной безопасностью	Стандарты управления информационной безопасностью. BS 7799 и ISO/IEC 17799. Их основные положения. Международный стандарт ISO/IEC 27001 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001.	ЛК, СЗ
		1.3	Создание СУИБ на предприятии	Этапы создания системы управления ИБ. Категорирование активов компании. Оценка защищенности информационной системы компании. Оценка информационных рисков.	ЛК, СЗ
		1.4	Методика оценки рисков информационной безопасности компании	Классификация системы рисков. Основные понятия. Управление рисками. Система минимизации рисков. Метод оценки рисков на основе модели угроз и уязвимостей.	ЛК, СЗ
		1.5	Методики и технологии управления рисками	Качественные методики управления рисками. Количественные методики управления рисками. Метод CRAMM. Разработка корпоративной методики анализа рисков.	ЛК, СЗ
		1.6	Постановка задачи	Методы оценивания информационных рисков. Табличные методы оценки рисков. Методика анализа рисков Microsoft.	ЛК, СЗ
		1.7	Обоснование необходимости инвестиций в информаци-онную безопасность компании	Методика FRAP. Методика OCTAVE. Методика RiskWatch.	ЛК, СЗ
		1.8	Обеспечение управления рисками ИБ	Документальная составляющая обеспечения. Внутренняя нормативная база организации в области управления рисками ИБ. Инструментальные средства управления рисками ИБ. Основные продукты и разработчики.	ЛК, СЗ
		1.9	Управление инцидентами ИБ	Определение инцидента информационной безопасности. Описание процедуры управления инцидентами безопасности на основе модели PDCA. Обнаружение и регистрация инцидента. Устранение причин, последствий инцидента и его расследование. Корректирующие и превентивные действия. Нормативная база процедуры управления ИТ-инцидентами. Стандарт ISO/IEC 20000.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
		1.10	Управление непрерывностью услуг	Задачи процесса управления непрерывностью услуг (ITSCM). Понятие процесса управления непрерывностью бизнеса (BCM). Планы обеспечения непрерывности бизнеса, обеспечения непрерывности и восстановления услуг. Жизненный цикл ITSCM. Анализ влияния на бизнес (BIA) процессов управления непрерывностью бизнеса. Анализ BIA как индикатор последствий потерь услуг для бизнеса. Построение диаграммы оценки влияния потери услуги или бизнес-процесса на бизнес в целом.	ЛК, СЗ

* - заполняется только по **ОЧНОЙ** форме обучения: *ЛК – лекции; ЛР – лабораторные работы; СЗ – практические/семинарские занятия.*

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 6.1. Материально-техническое обеспечение дисциплины

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
Лекционная	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническими средствами мультимедиа презентаций.	Персональный компьютер или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска.
Семинарская	Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и техническими средствами мультимедиа презентаций.	Персональные компьютеры или моноблоки с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет), проектор и экран, интерактивная или маркерная доска.
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	Персональный компьютер или моноблок с доступом к сети Интернет и прикладным ПО (веб-браузер, офисный пакет).

* - аудитория для самостоятельной работы обучающихся указывается **ОБЯЗАТЕЛЬНО**!

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Гришина, Н. В. Основы управления информационной безопасностью : учебно-методическое пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2021. — 99 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-110048-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1859951 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

2. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. - ISBN 978-5-9275-2742-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1021744 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

Дополнительная литература:

1. Вопросы управления информационной безопасностью: Учебное пособие для вузов. Основы управления информационной безопасностью / Курило А.П., Милославская

Н.Г., Сенаторов М.Ю. - Москва :Гор. линия-Телеком, 2013. - 244 с. (Вопросы управления информационной безопасностью)ISBN 978-5-9912-0271-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/560780 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

2. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И., - 2-е изд. - Москва :Гор. линия-Телеком, 2016. - 170 с.ISBN 978-5-9912-0363-0. - Текст : электронный. - URL: https://znanium.ru/catalog/product/560782 (дата обращения: 26.03.2026). – Режим доступа: по подписке.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров

- Электронно-библиотечная система РУДН – ЭБС РУДН https://mega.rudn.ru/MegaPro/Web
- ЭБС «Университетская библиотека онлайн» http://www.biblioclub.ru
- ЭБС Юрайт http://www.biblio-online.ru
- ЭБС «Консультант студента» www.studentlibrary.ru
- ЭБС «Знаниум» https://znanium.ru/

2. Базы данных и поисковые системы

- Sage https://journals.sagepub.com/
- Springer Nature Link https://link.springer.com/
- Wiley Journal Database https://onlinelibrary.wiley.com/
- Наукометрическая база данных Lens.org https://www.lens.org

Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля:*

1. Курс лекций по дисциплине «Основы управления информационной безопасностью».

* - все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины **в ТУИС**!

РАЗРАБОТЧИК:

Заведующий кафедрой информационной безопасности		Царегородцев Анатолий Валерьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой информационной безопасности		Царегородцев Анатолий Валерьевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой информационной безопасности		Царегородцев Анатолий Валерьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*