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

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
(код и наименование направления подготовки/специальности)

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

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Управление информационной безопасностью» входит в программу магистратуры «Управление информационной безопасностью» по направлению 10.04.01 «Информационная безопасность» и изучается в 3 семестре 2 курса. Дисциплину реализует Кафедра информационной безопасности . Дисциплина состоит из 1 раздела и 7 тем и направлена на изучение методов и средств управления информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объект

Целью освоения дисциплины является приобретение необходимого объема знаний и практических навыков по управлению информационной безопасностью, оценки рисков информационных ресурсов организации и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность; формирование представления о содержании процессов управления информационной безопасностью организации как результата внедрения системного подхода к решению задач обеспечения информационной безопасности

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Управление 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-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.2 Распределяет задачи на долго-, средне- и краткосрочные с обоснованием актуальности и анализа ресурсов для их выполнения;
УК-7	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных	УК-7.2 Проводит оценку информации, ее достоверность, строит логические умозаключения на основании поступающих информации и данных;
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Обосновывает требования к системе обеспечения информационной безопасности;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Управление 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 «Управление 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-7	Способен: искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач; проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающих информации и данных	Информационные базы данных; Разработка организационно-распорядительных документов по обеспечению информационной безопасности; Научно-исследовательская работа;	Научно-исследовательская работа; Преддипломная практика;
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	Научно-исследовательская работа; Управление проектами; Независимая оценка ИТ-компетенций (hh.ru);	Научно-исследовательская работа; Проектно-технологическая практика; Преддипломная практика; Информационно-психологическая безопасность; Независимая оценка ИТ-компетенций (hh.ru);
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	Теория игр и исследование операций; Защищенные информационные системы; Технологии обеспечения информационной безопасности;	Проектно-технологическая практика; Информационно-психологическая безопасность;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Управление информационной безопасностью» составляет «5» зачетных единиц.

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)**
			3
Контактная работа, ак.ч.	*102*		*102*
Лекции (**ЛК**)	34		34
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	68		68
Самостоятельная работа обучающихся, ак.ч.	*51*		*51*
Контроль (экзамен/зачет с оценкой), ак.ч.	*27*		*27*
Общая трудоемкость дисциплины	**ак.ч.**	***180***	*180*
	зач.ед.	***5***	*5*

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	Управление информационной безопасностью	1.1	Управление ИБ организации как процесс	Основные понятия, связанные с управлением ИБ Понятия: информационная безопасность, информационная безопасность объекта информатизации, безопасность информации, безопасность информационной технологии и их роль в процессах управления ИБ. Угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ. Сущность управления ИБ организации Необходимость управления обеспечением ИБ организации. Процессный подход к управлению ИБ. Системный подход к управлению ИБ. Управление обеспечением ИБ организации как процесс. Циклическая модель PDCA применительно к управлению ИБ.	ЛК, СЗ
		1.2	Планирование и организационно-распорядительные документы управления ИБ	Планирование в управлении ИБ. Определение приоритетов организации для разработки системы управления ИБ организации. Определение области действия системы управления ИБ организации. Определение защищаемых активов информационной инфраструктуры организации, их классификация. Разработка политики системы управления ИБ организации на основе характеристик бизнеса, организации, ее размещения, активов и технологий. Определение подхода к оценке риска в организации. Анализ и оценка рисков. Определение и оценка различных вариантов обработки рисков. Выбор целей и мер управления для обработки рисков.	ЛК, СЗ
		1.3	Стандарты в области управления ИБ	Роль стандартов в управлении ИБ. Основные организации, издающие стандарты по вопросам управления ИБ. Международная организация по стандартизации (ИСО, ISO). Международная электротехническая комиссия (МЭК, Национальные органы по стандартизации: Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Британский институт стандартов (BSI), Национальный институт стандартов и технологий США (NIST), Федеральное ведомство по безопасности информационных технологий (BSI, Германия). Общие сведения о стандартах США, Великобритании и Германии, касающихся вопросов	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				управления ИБ. Комплекс стандартов и рекомендаций Банка России по управлению ИБ. Общие требования к системам менеджмента ИБ. Нормы и правила менеджмента ИБ. Цели и меры управления. Организация обеспечения информационной безопасности. Области контроля. Международные стандарты по общим вопросам управления ИБ (ISO 27001, ISO 27002, ISO 27003) и гармонизированные с ними российские национальные стандарты.	
		1.4	Внутренние нормативные документы по управлению ИБ организации	Документационное обеспечение управления информационной безопасностью организации. Задачи и назначение документационного обеспечения управления информационной безопасностью организации. Иерархия внутренних нормативных документов по управлению информационной безопасностью организации. Требования к организации документационного обеспечения управления информационной безопасностью организации. Политика информационной безопасности организации. Роль политики ИБ как основного внутреннего нормативного документа по ИБ. Содержание политики ИБ. Жизненный цикл политики ИБ. Другие документы по управлению ИБ. Частные политики ИБ, их назначение и состав. Примеры областей обеспечения ИБ, управляемые частными политиками Документы, содержащие положения ИБ, применяемые к процедурам обеспечения ИБ. Документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ.	ЛК, СЗ
		1.5	Основные процессы СУИБ. Обязательная документация СУИБ	Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».	ЛК, СЗ
		1.6	Реализация системы управления ИБ	Планирование в управлении ИБ. Определение приоритетов	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
			организации	организации для разработки системы управления ИБ организации. Определение области действия системы управления ИБ организации. Определение защищаемых активов информационной инфраструктуры организации, их классификация. Разработка политики системы управления ИБ организации на основе характеристик бизнеса, организации, ее размещения, активов и технологий. Определение подхода к оценке риска в организации. Анализ и оценка рисков. Определение и оценка различных вариантов обработки рисков. Выбор целей и мер управления для обработки рисков. Внедрение системы управления информационной безопасностью. Разработка плана обработки рисков. Реализация плана обработки рисков для достижения намеченных целей управления. Внедрение мер управления, выбранные на стадии планирования, для достижения целей управления. Определение способа измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления. Реализация программы по обучению и повышению квалификации сотрудников. Управление работой системой управления ИБ организации. Управление ресурсами системы управления ИБ организации. Внедрение процедур и других мер управления, обеспечивающих быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ. Анализ системы управления ИБ организации. Выполнение процедуры мониторинга, контроля и анализа. Совершенствование системы управления ИБ организации. Выявление возможностей улучшения системы управления ИБ организации. Выполнение необходимых корректирующих и предупреждающих действий. Передача подробной информации о действиях по улучшению системы управления ИБ организации всем заинтересованным сторонам. Обеспечение внедрения улучшений системы управления ИБ организации для достижения запланированных целей.	
		1.7	Специальные вопросы управления ИБ организации	Управление информационной безопасностью финансовых организаций. Требования и рекомендации Банка России и	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				других регуляторов в сфере управления ИБ финансовых организаций. Комплекс СТО БР ИББС. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» и вопросы его использования. Вопросы ИБ индустрии платежных карт. Отдельные направления менеджмента ИБ. Менеджмент риска информационной безопасности. Менеджмент инцидентов информационной безопасности. Обеспечение непрерывности деятельности и восстановления после прерываний. Обеспечение ИБ на стадиях жизненного цикла автоматизированных систем. Критерии оценки безопасности информационных технологий и автоматизированных систем. Вопросы разработки сценариев по следующим различным ситуациям.	

* - 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.	Персональный компьютер или моноблок 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. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие : [16+] / Е. Н. Чекулаева, Е. С. Кубашева ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2020. – 156 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612591 (дата обращения: 16.04.2026). – Библиогр.: с. 127-129. – ISBN 978-5-8158-2165-1. – Текст : электронный.

2. Баланов, А. Н. Комплексная информационная безопасность : полный справочник специалиста : практическое пособие : [16+] / А. Н. Баланов. – Москва ; Вологда : Инфра-Инженерия, 2024. – 156 с. : табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=725651 (дата обращения: 16.04.2026). – ISBN 978-5-9729-1771-6. – Текст : электронный.

Дополнительная литература:

1. 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: 16.04.2026). – Режим доступа: по подписке.

2. Козырь, Н. С. Аудит информационной безопасности : учебник для вузов / Н. С. Козырь. — Москва : Издательство Юрайт, 2026. — 36 с. — (Высшее образование). — ISBN 978-5-534-20647-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590419 (дата обращения: 16.04.2026).

3. Козырь, Н. С. Оценка рисков и аудит информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 190 с. — (Высшее образование). — ISBN 978-5-534-17864-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590417 (дата обращения: 16.04.2026).

4. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2026. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2238628 (дата обращения: 16.04.2026). – Режим доступа: по подписке.

5. Золотарев, В. В. Управление информационной безопасностью. Ч. 1: Анализ информационных рисков : учебное пособие / В. В. Золотарев, Е. А. Данилова. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463037 (дата обращения: 16.04.2026). – Режим доступа: по подписке.

6. Жукова, М. Н. Управление информационной безопасностью. Ч. 2: Управление инцидентами информационной безопасности : учебное пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/463061 (дата обращения: 16.04.2026). – Режим доступа: по подписке.

7. 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: 16.04.2026). – 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 «Управление 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 безопасностью		Царегородцев Анатолий Валерьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

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

РУКОВОДИТЕЛЬ ОП ВО:

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