

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 22.05.2026 10:55:39

Уникальный программный ключ:

ca953a0120d891083f939673078ef1a989dae18a

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

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(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 «Аудит информационной безопасности» 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 7 семестре 4 курса. Дисциплину реализует Кафедра информационной безопасности. Дисциплина состоит из 1 раздела и 7 тем и направлена на изучение методов оценки состояния защищенности информационных систем, а также анализа эффективности применяемых мер защиты информации. В ходе изучения данной дисциплины студенты знакомятся с различными стандартами и методиками аудита, принципами организации и проведения проверок, а также с правовыми аспектами аудита информационной безопасности.

Целью освоения дисциплины является формирование у студентов теоретических знаний и практических навыков для проведения независимого аудита информационной безопасности организаций, выявления уязвимостей и недостатков в существующих системах защиты, а также разработки рекомендаций по их устранению и совершенствованию.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Аудит информационной безопасности» 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)
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; ОПК-17.2 Проводит аудит защищенности объекта информатизации в соответствии с нормативными документами;
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1 Знает методы и средства подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности; ОПК-8.2 Осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Аудит информационной безопасности» 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 «Аудит информационной безопасности».

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

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	Исследовательская практика; Ознакомительная практика; Эксплуатационная практика; Основы информационной безопасности (введение в специальность);	Технологическая практика;
ОПК-17	Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	Основы управления информационной безопасностью;	

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Аудит информационной безопасности» 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)
			7
<i>Контактная работа, ак.ч.</i>	68		68
Лекции (ЛК)	34		34
Лабораторные работы (ЛР)	0		0
Практические/семинарские занятия (СЗ)	34		34
<i>Самостоятельная работа обучающихся, ак.ч.</i>	22		22
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	18		18
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	Аудит информационной безопасности	1.1	Аудит информационной безопасности. Правовые и методологические основы аудита ИБ. Основные понятия.	Понятия «аудит информационной безопасности» и «критерии аудита информационной безопасности». Нормативно-правовая основа проведения аудита информационной безопасности. Факторы, влияющие на аудит информационной безопасности. Процессы проверки и оценки. Понятия «мониторинг и контроль защитных мер», «самооценка информационной безопасности», «внутренний аудит информационной безопасности» и «анализ функционирования». Проверяемые направления деятельности. Требования и действия при проведении аудита информационной безопасности. Принципы проведения аудита информационной безопасности. Методики оценки соответствия информационной безопасности финансовых организаций Российской Федерации.	ЛК, СЗ
		1.2	Процессы проверки системы обеспечения ИБ (СОИБ)	Виды проверок СОИБ. Мониторинг ИБ. Самооценка ИБ. Внутренний аудит ИБ. Цели и задачи внутренних аудитов ИБ. Организационные принципы внутреннего аудита ИБ. Принципы обеспечения эффективности внутреннего аудита ИБ. Подразделение внутреннего аудита, контролирующее вопросы ОИБ в организации. Внешний аудит ИБ. Принципы проведения внешнего аудита ИБ. Управление программой внешнего аудита ИБ. Компетентность аудиторов ИБ. Взаимоотношения представителей аудиторской группы и проверяемых организаций. Анализ СОИБ со стороны высшего руководства организации. Инструментальные средства проверки ИБ.	ЛК, СЗ
		1.3	Внешний аудит информационной безопасности	Понятия «внешний аудит информационной безопасности», «соответствие» и «несоответствие» критериям аудита информационной безопасности. Стороны проведения аудита – «заказчик» и «исполнитель» аудита. Цели, программа и план внешнего аудита информационной безопасности. Последовательность процессов менеджмента программы внешнего аудита информационной безопасности, основные направления проверки при внешнем аудите информационной безопасности. Внедрение, контроль и анализ программы	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				внешнего аудита информационной безопасности. Этапы проведения внешнего аудита информационной безопасности. Понятие «свидетельство аудита информационной безопасности», источники свидетельств аудита информационной безопасности. Результаты проведения внешнего аудита информационной безопасности и правила их согласования. Контроль за деятельностью аудиторов информационной безопасности. Риски внешнего аудита информационной безопасности. Понятие «компетентность аудитора».	
		1.4	Критерии аудита информационной безопасности. Национальные стандарты управления информационной безопасностью.	Стандарты по обеспечению безопасности информационных технологий в России. Практика оценки соответствия организаций российским стандартам. Отраслевые российские стандарты по обеспечению информационной безопасности. Комплекс документов по стандартизации информационной безопасности Банка России СТО БР ИББС. Обеспечение информационной безопасности критической инфраструктуры. Реализация требований по информационной безопасности на основе приказов и методических материалов ФСТЭК, ФСБ и Банка России. Реализация требований по оценке состояния информационной безопасности финансовых организаций на основе стандартов серии ГОСТ Р 57580.x.	ЛК, СЗ
		1.5	Критерии аудита информационной безопасности. Международные стандарты управления информационной безопасностью	Международные стандарты по обеспечению безопасности информационных технологий, применяемые в России. Стандарты серии ГОСТ Р ИСО/МЭК 27xxx. Стандарт безопасности данных индустрии платежных карт PCI DSS, его назначение, роль и место. Основная цель достижения соответствия требованиям стандарта PCI DSS. Методы проверки соответствия требованиям стандарта PCI DSS. Понятия «торгово-сервисное предприятие», «поставщик услуг» и «квалифицированный аудитор безопасности (QSA)». Разделы требований PCI DSS по обеспечению информационной безопасности. Результаты аудита соответствия информационной инфраструктуры требованиям PCI DSS. Этапы процесса проведения оценки соответствия PCI DSS.	ЛК, СЗ
		1.6	Непрерывность бизнеса и её аудит	Понятия «непрерывность бизнеса», «бесперебойность бизнеса»,	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				«менеджмент непрерывности бизнеса». Виды и примеры воздействия катастроф. Компоненты процесса непрерывности бизнеса. Политика непрерывности бизнеса, оценка влияния, анализ критичности, стратегия и планы непрерывности функционирования и восстановления. Определение задач по восстановлению, понятия «целевое время восстановления», «точка восстановления». Технологии обеспечения устойчивости и восстановления. Компоненты программы менеджмента непрерывностью бизнеса. Проверка планов и процедур непрерывности функционирования и восстановления. Понятие «система управления непрерывностью бизнеса». Задачи аудита менеджмента непрерывности бизнеса, определение эффективности плана менеджмента непрерывностью бизнеса.	
		1.7	Методы тестирования информационной безопасности.	Инструментальные средства тестирования Понятия «обследование», «интервью» и «тестирование». Подготовка и практика интервьюирования. Методы тестирования: тестирование «вслепую», «дважды слепое» тестирование, тестирование методом «серого ящика», тестирование методом «двойного серого ящика», тестированием методом «тандема», реверсивное тестирование. Требования к инструментальным средствам тестирования. Объекты тестирования инструментальных средств. Системы анализа защищенности, системы сбора и корреляции событий безопасности. Тестирование на проникновение.	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. 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: 27.03.2026).

2. Аверченков, В. И. Аудит информационной безопасности : учебное пособие для вузов / В. И. Аверченков. - 4-е изд., стер. - Москва : ФЛИНТА, 2021. - 269 с. - ISBN 978-5-9765-1256-6. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1843184> (дата обращения: 27.03.2026). – Режим доступа: по подписке.

Дополнительная литература:

1. Казакова, Н. А. Аудит : учебник для вузов / Н. А. Казакова, Е. И. Ефремова ; под общей редакцией Н. А. Казаковой. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 422 с. — (Высшее образование). — ISBN 978-5-534-21846-6. — Текст :

электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/582286> (дата обращения: 27.03.2026).

2. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для вузов / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2026. — 157 с. — (Высшее образование). — ISBN 978-5-534-17866-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/590420> (дата обращения: 27.03.2026).

3. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2024. — 602 с. — (Высшее образование). - ISBN 978-5-16-019904-7. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2021464> (дата обращения: 27.03.2026). – Режим доступа: по подписке.

4. Нормативное сопровождение информационной безопасности : учебное пособие / С. И. Фокина, А. В. Выволокина, А. Ю. Гарькушев, А. В. Липис. – Москва ; Вологда : Инфра-Инженерия, 2025. - 136 с. – ISBN 978-5-9729-2530-8. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2225338> (дата обращения: 27.03.2026). – Режим доступа: по подписке.

5. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебник для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2026. — 170 с. — (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/589310> (дата обращения: 27.03.2026).

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/>

- Научометрическая база данных Lens.org <https://www.lens.org>

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

1. Курс лекций по дисциплине «Аудит информационной безопасности».

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

РАЗРАБОТЧИК:

Заведующий кафедрой
информационной безопасности

Должность, БУП

Подпись

Царегородцев Анатолий
Валерьевич

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой
информационной безопасности

Должность БУП

Подпись

Царегородцев Анатолий
Валерьевич

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой
информационной безопасности

Должность, БУП

Подпись

Царегородцев Анатолий
Валерьевич

Фамилия И.О.