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

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

(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 «Комплексное обеспечение защиты информации объекта информатизации» 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 8 семестре 4 курса. Дисциплину реализует Кафедра информационной безопасности . Дисциплина состоит из 1 раздела и 6 тем и направлена на изучение методов и технологий комплесного обеспечения информационной безопасности организаций. Студенты изучают подходы к созданию комплексной системы защиты информации, включающей организационные, правовые, технические и программно-аппаратные меры и средства, а также механизмы мониторинга и реагирования на инциденты информационной безопасности.

Целью освоения дисциплины является формирование у обучающихся понимания процессов и базовых навыков проектирования, внедрения и поддержки комплексной системы защиты информации организации на основе принципов баланса между безопасностью и функциональностью защищемых систем, минимизации рисков утраты, модификации или несанкционированного доступа к данным.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Комплексное обеспечение защиты информации объекта информатизации» 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-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1 Знает методики подготовки исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений; ОПК-12.2 Проводит подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;
ОПК-14	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	ОПК-14.1 Знает возможные функциональные процессы объекта защиты и его информационных составляющих для выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба; ОПК-14.2 Проводит анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;
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;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Комплексное обеспечение защиты информации объекта информатизации» 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 «Комплексное обеспечение защиты информации объекта информатизации».

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-12	Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	Эксплуатационная практика; Экономика защиты информации;	
ОПК-14	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	Эксплуатационная практика; Аппаратные средства вычислительной техники; Защита информации от утечки по техническим каналам; Физические основы защиты информации; Анализ и управление рисками информационной безопасности; Программно-аппаратные средства защиты информации;	
ОПК-16	Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	Основы управления информационной безопасностью; Эксплуатационная практика;	

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Комплексное обеспечение защиты информации объекта информатизации» 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)**
			8
Контактная работа, ак.ч.	*80*		*80*
Лекции (**ЛК**)	40		40
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	40		40
Самостоятельная работа обучающихся, ак.ч.	*64*		*64*
Контроль (экзамен/зачет с оценкой), ак.ч.	*36*		*36*
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	Комплексное обеспечение защиты информации объекта информатизации	1.1	Выявление уязвимых элементов, через которые возможна реализация угроз информационной безопасности предприятия	Роль и место защиты информации в обеспечении информационной безопасности. Информационная безопасность: сущность и содержание. Угрозы информационной безопасности и условия их нейтрализации. Понятие об информационном объекте и его элементах. Объекты, методы и система обеспечения информационной безопасности. Защита информации в обеспечении информационной безопасности и ее задачи. Основы формирования системы обеспечения информационной безопасности и комплексной системы защиты информации. Организационные основы обеспечения информационной безопасности. Условия и факторы, оказывающие влияние на организационную структуру системы обеспечения информационной безопасности. Требования международных стандартов по вопросам организации обеспечения информационной безопасности. Принципы организационного обеспечения информационной безопасности. Силы и средства обеспечения информационной безопасности.	ЛК, СЗ
		1.2	Принципы организации комплексной системы защиты информации (КСЗИ) на предприятии и этапы разработки	Принципы организации КСЗИ и требования к защищенности АСУ. Классификация АСУ по защищенности от несанкционированного доступа. Разработка комплексной системы защиты информации на предприятии. Разработка проекта и определение задач администрации по внедрению системы обеспечения информационной безопасности и защиты информации. Внедрение комплексной системы защиты информации на предприятии. Аттестация систем защиты и обучение пользователей.	ЛК, СЗ
		1.3	Технологическое, организационное, кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ на предприятии	Технологическое обеспечение функционирования КСЗИ. Процессный подход к обеспечению информационной безопасности. Модель Деминга-Шухарта как основа организации процесса обеспечения информационной безопасности. Стандарты, базирующиеся на процессном подходе к обеспечению информационной безопасности (ISO	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				27001) и Стандарт Банка России СТО БР ИББС 1.0. Организационные основы обеспечения информационной безопасности и КСЗИ. Принципы организационного обеспечения информационной безопасности и структура системы обеспечения. Силы обеспечения информационной безопасности. Роль подразделения защиты информации в системе обеспечения информационной безопасности. Средства обеспечения информационной безопасности предприятия. Технологии обеспечения информационной безопасности и роли в системе ее обеспечения руководства предприятием и службы обеспечения информационной безопасности. Кадровое обеспечение предприятия в комплексной системе защиты информации. Направления и методы работы с персоналом в интересах защиты информации. Проверочные мероприятия, обучение работе с конфиденциальной информацией и оформление допуска к ней при приеме на работу. Мониторинг осведомленности персонала о тайнах работодателя. Правовое обеспечение информационной безопасности. Правовые нормы в обеспечении информационной безопасности. Право и его роль в регулировании комплекса отношений в информационной сфере. Отрасли права, обеспечивающие законность в интересах информационной безопасности. Структура и направленность правовых мер обеспечения информационной безопасности. Материально-техническое обеспечение функционирования КСЗИ. Инвентаризация информационных ресурсов компании. Сертифицированные программно-аппаратные средства защиты информации. Практические рекомендации по выбору и использованию средств защиты.	
		1.4	Каналы несанкционированного доступа к информации предприятия через Интернет	Обеспечение информационной безопасности предприятия в Интернет-коммуникациях. Угрозы безопасности, связанные с подключением компании к сети Интернет. Внешние угрозы интернет-порталу. Подсистемы КСЗИ: разграничения доступа к ресурсам портала, обнаружения и предотвращения сетевых атак, контроля целостности, межсетевого экранирования. Обеспечение защищённого подключения к Интернет на основе	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				сервера терминальных служб. Методы организации защищённого подключения к Интернету на основе наложенных средств защиты. Аудит интернет-узлов компаний (penetration testing), направленный на оценку соответствия системы управления информационной безопасностью требованиям стандарта ISO 27001. Обеспечение безопасности электронного документооборота. Создание защищённой системы электронного документооборота на основе технологии инфраструктуры открытого ключа. Удостоверяющий центр как основа для управления цифровыми сертификатами пользователя. Использование USB-ключей eToken в качестве хранилища цифровых сертификатов и секретных ключей пользователей.	
		1.5	Модели оценки угроз информационной безопасности и оценка эффективности функционирования КСЗИ на предприятии	Угрозы информационной сфере предприятия и уязвимости ее объектов. Внутренние угрозы безопасности информации, связанные с действием «инсайдеров». Вирусные угрозы. Внешние атаки из сети Интернет. Спам. Уязвимости информационных объектов. Содержание и методика оценки рисков КЗИ. Содержание понятия «риски» и технологии их анализа в интересах защиты информации. Понятие качественной и количественной оценки рисков, шкалы и критерии измерения. Комплексная оценка рисков безопасности и ее основные этапы. Особенности применения инструментальных средств оценки рисков на примере программного комплекса MSAT (Microsoft Security Assessment Tool). Критерии оценки уровня информационной безопасности предприятия. Методика оценки рисков OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation). Оценка текущего состояния информационной безопасности компании. Модели оценки угроз безопасности КСЗИ. Организация и проведение аудита безопасности АСУ. Сущность и содержание аудита, направленного на оценку соответствия системы управления информационной безопасностью требованиям стандарта ISO 27001. Требования COBIT в реализации аудита информационной безопасности. Инструментальные средства анализа информационной безопасности.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
		1.6	Создание политик безопасности	Политики информационной безопасности. Содержание политики информационной безопасности. Политики безопасности информационно-телекоммуникационных технологий. Особенности выработки официальной политики предприятия в области информационной безопасности и управления безопасностью. Инциденты и эскалации в практике КЗИ. Инциденты и реагирование на них. Эскалации в практике защиты информации.	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. Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588741 (дата обращения: 31.03.2026).

2. Петровский, М. В. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. - Москва ; Вологда : Инфра-Инженерия, 2024. - 144 с. - ISBN 978-5-9729-1610-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2169702 (дата обращения: 07.04.2026). – Режим доступа: по подписке.

3. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. -

URL: https://znanium.ru/catalog/product/1843022 (дата обращения: 07.04.2026). – Режим доступа: по подписке.

Дополнительная литература:

1. Методы и средства комплексной защиты информации в технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. - Саров : РФЯЦ-ВНИИЭФ, 2019. - 224 с. - ISBN 978-5-9515-0429-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1230827 (дата обращения: 07.04.2026). – Режим доступа: по подписке.

2. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583236 (дата обращения: 07.04.2026).

3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2026. — 349 с. — (Высшее образование). — ISBN 978-5-534-19762-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583858 (дата обращения: 31.03.2026).

4. Макаренко, С. И. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем : учебное пособие / С. И. Макаренко, А. А. Ковальский, С. А. Краснов. — Санкт-Петербург : Наукоемкие технологии, 2020 — Часть 2 : Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях — 2020. — 357 с. — ISBN 978-5-6044429-8-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/329378 (дата обращения: 31.03.2026). — Режим доступа: для авториз. пользователей.

5. Помазанов, А. В. Защита информации от утечки по техническим каналам : учебное пособие / А. В. Помазанов ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2024. - 134 с. – ISBN 978-5-9275-4851-4. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2220025 (дата обращения: 01.04.2026). – 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 «Комплексное обеспечение защиты информации объекта информатизации».

* - 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.*