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)

2025 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 прикладного искусственного интеллекта. Дисциплина состоит из 1 раздела и 6 тем и направлена на изучение методов и технологий, обеспечивающих всестороннюю защиту информации в информационных системах и сетях. Студенты изучают подходы к созданию комплексной системы защиты информации, включающей организационные, правовые, технические и программные меры, а также механизмы мониторинга и реагирования на инциденты информационной безопасности.

Целью освоения дисциплины является одготовка специалистов, способных проектировать, внедрять и поддерживать комплексную систему защиты информации на объектах информатизации, обеспечивая баланс между безопасностью и функциональностью информационных систем, а также минимизировать риски 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)
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует поставленную задачу, выделяя ее базовые составляющие, определяет и ранжирует информацию, требуемую для её решения; УК-1.2 Осуществляет поиск информации для решения поставленной задачи по различным типам запросов, предлагает варианты её решения и анализирует возможные последствия их использования;
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Определяет связи между поставленными задачами и ожидаемые результаты их решений, которые напрямую связаны с достижением цели проекта; УК-2.2 В рамках поставленных задач определяет имеющиеся ресурсы, ограничения и действующие правовые нормы;
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.2 Принимает участие в формировании политики информационной безопасности, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации на объекте защиты;
ОПК-12	Способен проводить подготовку исходных данных для проектирования подсистем,	ОПК-12.1 Знает методики подготовки исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	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-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.2 Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.2 При решении профессиональных задач организует защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ОПК-8	Способен осуществлять подбор, изучение и обобщение 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;
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1 Применяет средства криптографической защиты информации для решения задач профессиональной деятельности; ОПК-9.2 Применяет средства технической защиты информации для решения задач профессиональной деятельности;

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*

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	Ознакомительная практика; Эксплуатационная практика; Исследовательская практика; *Специальные разделы математики (методы оптимизации)***; *Моделирование процессов и систем защиты информации***; *Методы принятия решений***; *Теория систем и системный анализ***; Правоведение; Организационное и правовое обеспечение информационной безопасности;	
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Ознакомительная практика; Эксплуатационная практика; Исследовательская практика; Информатика; *Специальные разделы математики (методы оптимизации)***; *Моделирование процессов и систем защиты информации***; *Методы принятия решений***; *Теория систем и системный анализ***; Информационные технологии;	
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Эксплуатационная практика; Организационное и правовое обеспечение информационной безопасности; Защищенный документооборот; Программно-аппаратные средства защиты информации;	
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	Ознакомительная практика; Эксплуатационная практика; Исследовательская практика; Организационное и правовое обеспечение информационной безопасности; Защищенный документооборот;	
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов	Исследовательская практика; Ознакомительная практика; Эксплуатационная практика; Информационные технологии; Организационное и правовое обеспечение информационной	

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
	в целях решения задач профессиональной деятельности	безопасности; Основы информационной безопасности (введение в специальность);	
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	Методы и средства криптографической защиты информации; Аппаратные средства вычислительной техники; Защита информации от утечки по техническим каналам; Физические основы защиты информации; Эксплуатационная практика;	
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	Эксплуатационная практика; Организационное и правовое обеспечение информационной безопасности; Защита информации от утечки по техническим каналам;	
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;	
	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	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; Эксплуатационная практика; Организационное и правовое обеспечение информационной безопасности; 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 «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	Содержание раздела (темы)		Вид учебной работы*
Раздел 1	Комплексное обеспечение защиты информации объекта информатизации	1.1	Выявление уязвимых элементов, через которые возможна реализация угроз инфор-мационной безопасности предприятия	ЛК, СЗ
		1.2	Принципы организации КСЗИ на предприятии и этапы разработки	ЛК, СЗ
		1.3	Технологическое, организационное, кадровое, материально-техническое и норма-тивно-методическое обеспечение функционирования КСЗИ на предприятии.	ЛК, СЗ
		1.4	Каналы несанкционированного доступа к информации предприятия через Интернет.	ЛК, СЗ
		1.5	Модели оценки угроз информационной безопасности и оценка эффективности функ-ционирования КСЗИ на предприятии.	ЛК, СЗ
		1.6	Создание политик безопасности.	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.	
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.	
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.	

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Доктрина информационной безопасности Российской Федерации, 2016 г.

2. «Стратегия национальной безопасности Российской Федерации до 2020 г.». Указ Прези-дента РФ №537 от 12.05.2009

3. Федеральный закон № 5485-1 «О государственной тайне», 21 июля 1993 г. (с изм. от 6.10.97 г. и от 11.12.2011 г.), – М.: МВК по ЗГТ, 2011.

4. Постановление правительства РФ «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в ФОИВ» № 1233 от 03 ноября 1994 г. – М.: МВК по ЗГТ, 1998.

5. Постановление правительства РФ «Об утверждении правил отнесения сведений к раз-личным степеням секретности» № 170 от 20 февраля 1995 г. – М.: МВК по ЗГТ, 1998.

6. Инструкция о порядке допуска должностных лиц и граждан РФ к государственной тайне. Постановление Правительства РФ от 6 февраля 2010 г. № 63.

7. Международный стандарт ИСО/МЭК 27001. Первое издание 2005-10-15. Информацион-ные технологии. Методы защиты. Системы менеджмента защиты информации.

8. Международный стандарт ISO/IEC 27002:2005(E) «Информационные технологии. Свод правил по управлению защитой информации».

9. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.

10. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

11. ГОСТ Р ИСО/МЭК 13335-1-2006 «Методы и средства обеспечения безопасности. Ч. 1. Концепция и модели менеджмента безопасности информационных и телекоммуникаци-онных технологий».

12. ОСТ 45.127-99 «Система обеспечения информационной безопасности взаимоувязанной сети связи РФ. Термины и определения».

13. ГОСТ Р 50995.0.1-96. Технологическое обеспечение создания продукции, 1.07.97 г.

14. ГОСТ Р ИСО/МЭК ТО 18044-2007. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

15. Британский стандарт BS 25999-1:2006. Управление непрерывностью бизнеса – Ч.1: Прак-тические правила.

16. Герасименко В.А., Малюк А.А. Основы защиты информации. Учебник. – М.: МИФИ, 1997. – 537 с.

17. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Ака-демический Проект; Фонд «Мир», 2003.

Дополнительная литература:

1. Бондарев В. В. Проблемы подготовки специалистов в области информационной безопас-ности. Материалы 2-й Межрегиональной конференции «Информационная безопасность регионов России», СПб, 2001.

2. Стрельцов А.А. Информационная безопасность Российской Федерации. - М.: Высшая школа, 2003. С. 27-48

3. Садердинов А.А. Информационная безопасность предприятия. Уч. пособие. – М.: Даш-ков и Ко, 2004.

4. Курносов Ю.В., Конотопов П.Ю. Аналитика: методология, технология и организация информационно-аналитической работы. – М.: Издательство «Русаки», 2004.

5. С. Петренко. Политики безопасности компании при работе в Internet. http://citforum.ru/security/internet/security_pol/

6. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность/Петренко С. А., Симонов С. В. - М.: Компания АйТи; ДМК Пресс, 2004. - 384 с.

7. Пугачев В.П. Руководство персоналом организации: Учебник (Серия «Управление пер-соналом»). – М.: Аспект Пресс, 2002. – 279 с.

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:

Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой		Подолько Павел Михайлович [М|] заведующий кафедрой
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Должность, БУП	*Подпись*	*Фамилия И.О.*