**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;<br>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;<br>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 | ОПК-12.1 Знает методики подготовки исходных данных для проектирования подсистем, средств обеспечения защиты |

| Шифр | Компетенция | Индикаторы достижения компетенции (в рамках данной дисциплины) |
|---|---|---|
| | для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений | информации и для технико-экономического обоснования соответствующих проектных решений;<br>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;<br>ОПК-9.2 Применяет средства технической защиты информации для решения задач профессиональной деятельности; |
| пОПК-2.1 | 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 | пОПК-2.1.2 Проводит анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных<br>источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба |
| пОПК-2.2 | Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его<br>информационных составляющих с целью повышения их устойчивости | пОПК-2.2.2 Формирует предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных<br>составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы |

| Шифр | Компетенция | Индикаторы достижения компетенции (в рамках данной дисциплины) |
|---|---|---|
| | к деструктивным воздействиям на информационные ресурсы | |
| пОПК-2.3 | Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности | пОПК-2.3.2 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* |
|---|---|---|---|
| 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* | |

| Шифр | Наименование компетенции | Предшествующие дисциплины/модули, практики* | Последующие дисциплины/модули, практики* |
|---|---|---|---|
| | | *анализ***;<br>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;<br>Организационное и правовое обеспечение информационной безопасности;<br>Защищенный документооборот;<br>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;<br>Эксплуатационная практика;<br>Исследовательская практика;<br>Организационное и правовое обеспечение информационной безопасности;<br>Защищенный документооборот; | |
| ОПК-8 | Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности | Исследовательская практика;<br>Ознакомительная практика;<br>Эксплуатационная практика;<br>Информационные технологии;<br>Организационное и правовое обеспечение информационной безопасности;<br>Техническая документация в ИТ-проектах;<br>Основы информационной безопасности (введение в специальность);<br>Второй иностранный язык в сфере профессиональной коммуникации;<br>*Иностранный язык в сфере профессиональной коммуникации***;<br>*Русский язык как иностранный в сфере профессиональной коммуникации***; | |
| ОПК-9 | Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности | Методы и средства криптографической защиты информации;<br>Аппаратные средства вычислительной техники;<br>Защита информации от утечки по техническим каналам;<br>Физические основы защиты информации;<br>Эксплуатационная практика; | |

| Шифр | Наименование компетенции | Предшествующие дисциплины/модули, практики* | Последующие дисциплины/модули, практики* |
|---|---|---|---|
| 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;<br>Организационное и правовое обеспечение информационной безопасности;<br>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;<br>Экономика защиты информации;<br>Техническая документация в ИТ-проектах; | |
| пОПК-2 | 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;<br>Защита информации от утечки по техническим каналам;<br>Физические основы защиты информации;<br>Анализ и управление рисками информационной безопасности;<br>Программно-аппаратные средства защиты информации;<br>Эксплуатационная практика;<br>Организационное и правовое обеспечение информационной безопасности;<br>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 «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)** |
|---|---|---|---|
| | | | **8** |
| *Контактная работа, ак.ч.* | *64* | | *64* |
| Лекции (**ЛК**) | 32 | | 32 |
| Лабораторные работы (**ЛР**) | 0 | | 0 |
| Практические/семинарские занятия (**СЗ**) | 32 | | 32 |
| *Самостоятельная работа обучающихся, ак.ч.* | *17* | | *17* |
| *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 | 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 | Лекционный класс для практической подготовки, проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. | Комплект специализированной мебели: учебная доска; технические средства: Интерактивная панель 86 дюймов HUAWEI idea Hub S2 IHS2-86SA со встраиваемым OPS компьютером HUAWEI в комплекте с подвижной подставкой HUAWEI idea Hub White Rolling Stand _25, Двух объективная PTZ-видеокамера Nearity V520d, Системный блок CPU Intel Core I9-13900F/MSI PRO Z790-S Soc-1700 Intel Z790 / Samsung DDR5 16GB DIMM 5600MHz 2шт/ Samsung SSD 1Tb /Видеокарта RTX3090 2; Монитор LCD LG 27" 27UL500-W белый IPS 3840x2160 5ms 300cd 1000:1 (Mega DCR) DisplayPort P HDMIx2 Audioout, vesa. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/Office 365, Teams, Skype). Количество посадочных мест - 28. |
| Семинарская | Лекционный класс для практической подготовки, проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. | Комплект специализированной мебели: учебная доска; технические средства: Интерактивная панель 86 дюймов HUAWEI idea Hub S2 IHS2-86SA со встраиваемым OPS компьютером HUAWEI в комплекте с подвижной подставкой HUAWEI idea Hub White Rolling Stand _25, Двух объективная PTZ-видеокамера Nearity V520d, Системный блок CPU Intel Core I9-13900F/MSI PRO Z790-S Soc-1700 Intel Z790 / Samsung DDR5 16GB DIMM 5600MHz 2шт/ Samsung SSD 1Tb /Видеокарта RTX3090 2; Монитор LCD LG 27" 27UL500-W белый IPS 3840x2160 5ms 300cd 1000:1 (Mega DCR) DisplayPort P HDMIx2 Audioout, vesa. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/Office |

| | | |
|---|---|---|
| | | 365, Teams, Skype). Количество посадочных мест - 28. |
| 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. | Компьютерный класс для практической подготовки, проведения занятий практико-лабораторного характера, самостоятельной работы, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации<br>Комплект специализированной мебели; учебная доска; технические средства: Моноблок HP ProOne 440 Intel I5 10500T/8 GB/256 GB/audio, монитор 24"; Мультимедиа проектор Casio XJ-V100W; Экран, моторизованный Digis Electra 200*150 Dsem-4303<br>Программное обеспечение: Продукты Microsoft (MS Windows, MS Office) – подписка Enrollment for Education Solution (EES) №56278518 от 23.04.2019 |
| | | Компьютерный класс - учебная аудитория для практической подготовки, лабораторно-практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также самостоятельной работы<br>Комплект специализированной мебели; (в т.ч. электронная доска); мультимедийный проектор BenqMP610; экран моторизованный Sharp 228*300; доска аудиторная поворотная; Комплект ПК iRU Corp 317 TWR i7 10700/16GB/ SSD240GB/2TB 7.2K/ GTX1660S-6GB /WIN10PRO64/ BLACK + Комплект Logitech Desktop MK120, (Keybord&mouse), USB, [920-002561] + Монитор HP P27h G4 (7VH95AA#ABB) (УФ-000000000059453)-5шт., Компьютер Pirit Doctrin4шт., ПО для ЭВМ LiraServis Academic Set 2021 Состав пакета ACADEMIC SET: программный комплекс "ЛИРА-САПР FULL". программный комплекс "МОНОМАХ-САПР PRO". программный комплекс "ЭСПРИ. |

* - 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 http://lib.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 «Троицкий мост»

2. Базы данных и поисковые системы

- электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/
- поисковая система Яндекс https://www.yandex.ru/
- поисковая система Google https://www.google.ru/
- реферативная база данных SCOPUS http://www.elsevierscience.ru/products/scopus/

*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**!

## 8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

Оценочные материалы и балльно-рейтинговая система* оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Комплексное обеспечение защиты информации объекта информатизации» представлены в Приложении к настоящей Рабочей программе дисциплины.

* - ОМ и БРС формируются на основании требований соответствующего локального нормативного акта РУДН.