

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Наумова Наталия Александровна
Должность: Ректор
Дата подписания: 21.10.2026 10:14:12
Уникальный программный ключ:
6b5279da4e034f5e3a120a50c43c09e2

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ»
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ)

Факультет безопасности жизнедеятельности
Кафедра безопасности жизнедеятельности и методики обучения

Согласовано
деканом факультета безопасности
жизнедеятельности

«11» марта 2026 г.

/Ковалев П.А.

Рабочая программа дисциплины

Безопасность информационного пространства

Направление подготовки

44.04.01 Педагогическое образование

Программа подготовки:

Безопасность образовательных организаций

Квалификация

Магистр

Форма обучения

Очно-заочная

Согласовано учебно-методической комиссией
факультета безопасности жизнедеятельности
Протокол «24» марта 2026 г. № 7
Председатель УМКом

/Ковалев П.А.

Рекомендовано кафедрой безопасности
жизнедеятельности и методики обучения
Протокол «02» марта 2026 г. № 7
Зав. кафедрой

/Махонин Е.В./

Москва
2026

Авторы-составители:
Ковалев П.А., кандидат психологических наук

Рабочая программа дисциплины «Безопасность информационного пространства» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 44.04.01 Педагогическое образование, утвержденного приказом МИНОБРНАУКИ РОССИИ от 22.02.2018 № 126.

Дисциплина входит в Модуль "Технологии управления безопасностью образовательной организации" в часть, формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)» и является обязательной для изучения.

Реализуется в формате электронного обучения с применением дистанционных образовательных технологий

Год начала подготовки (по учебному плану) 2026 г.

Содержание:

1. Планируемые результаты обучения	4
2. Место дисциплины в структуре образовательной программы	4
3. Объем и содержание дисциплины	4
4. Учебно-методическое обеспечение самостоятельной работы обучающихся	9
5. Фонд оценочных средств для проведения текущей и промежуточной аттестации по дисциплине	10
6. Учебно-методическое и ресурсное обеспечение дисциплины	17
7. Методические указания по освоению дисциплин	18
8. Информационные технологии для осуществления образовательного процесса по дисциплине	19
9. Материально-техническое обеспечение дисциплины	19

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

1.1 Цель и задачи дисциплины

Целью изучения дисциплины «Безопасность информационного пространства» является формирование у магистрантов системных представлений о современных угрозах и рисках в цифровом контуре образовательной организации, а также развитие профессиональных компетенций по проектированию, внедрению и управлению комплексной системой информационной безопасности.

Задачи дисциплины:

- освоение основных принципов и подходов по созданию информационной безопасности образовательной организации, как части управления системой комплексной безопасности;
- развитие практических навыков по управлению информационной безопасностью образовательных организаций;
- формирование навыков инициировать, планировать и организовывать работу в образовательных организациях в соответствии с целями и задачами государственной политики в области комплексной безопасности образовательных организаций.

1.2 Планируемые результаты обучения

В результате освоения дисциплины у обучающегося формируются следующие компетенции:

ДПК-1. Способен обеспечивать и поддерживать доступность ресурсов учебного пространства и услуг, создание защищенной физической и психологической среды, способствующей успешной реализации образовательных целей и задач всеми участниками образовательного процесса;

ДПК-4. Способен осуществлять управление созданием безопасных условий обучения и воспитания, организации питания обучающихся и работников, обеспечению охраны их здоровья.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в Модуль "Технологии управления безопасностью образовательной организации" в часть, формируемую участниками образовательных отношений Блока 1 «Дисциплины (модули)» и является обязательной для изучения.

Дисциплина «Безопасность информационного пространства» является основой для успешного освоения всех дисциплин Модуля, в том числе «Антитеррористическая и антиэкстремистская защищенность образовательных организаций», «Социальная безопасность и профилактика девиантного поведения» «Мониторинг и аудит безопасности» и направлена на подготовку компетентных специалистов, способных эффективно управлять процессами обеспечения безопасности, учитывая управленческие навыки прогнозирования рисков и управления рисками.

3. ОБЪЕМ И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Объем дисциплины

Показатель объема дисциплины	Форма обучения
	Очно-заочная
Объем дисциплины в зачетных единицах	3
Объем дисциплины в часах	108
Контактная работа:	26,3

Лекции	8 ¹
Практические занятия	16 ¹
Контактные часы на промежуточную аттестацию:	2,3
Предэкзаменационная консультация	2 ¹
Экзамен	0,3
Самостоятельная работа	72 ¹
Контроль	9,7

Форма промежуточной аттестации является: экзамен в 4 семестре.

3.2 Содержание дисциплины

Наименование разделов (тем) дисциплины с кратким содержанием	Кол-во часов	
	Лекции	Практические занятия
Раздел 1: Теоретико-методологические основы и нормативно-правовые регулирование безопасности информационного пространства	4	8
Тема 1. Концептуализация понятия «информационное пространство» и парадигма угроз в цифровой среде Эволюция понятийного аппарата: от защиты информации к обеспечению безопасности цифрового периметра образовательной организации (EdTech Security). Архитектура современного информационного пространства образовательной организации. Цифровая экосистема как объект управления и защиты. Классификация угроз информационной безопасности организации. Актуальные киберугрозы для сферы образования. Угрозы утечки персональных данных участников образовательного процесса. Концепция "нулевого доверия" в контексте обеспечения кибербезопасности образовательной организации. Управление цифровыми репутационными рисками. Психологическая безопасность в цифровой среде. Профилактика кибербуллинга, троллинга и других форм онлайн-агрессии среди обучающихся. Экономические аспекты кибербезопасности. Взаимосвязь физической и информационной безопасности.	2	4
Тема 2. Нормативно-правовой ландшафт и институциональные механизмы регулирования Федеральный закон № 152-ФЗ «О персональных данных»: ключевые требования к операторам ПДн в системе образования. Нормативные акты ФСТЭК России и ФСБ России. Требования по защите информации в государственных информационных системах (КИИ). Законодательство об образовании об обязанности образовательной организации по созданию безопасных условий обучения. Требования к использованию отечественного ПО. Правовое регулирование применения систем контент-фильтрации. Ответственность должностных лиц за нарушение требований инфор-	2	4

¹ Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

мационной безопасности. Документальное обеспечение системы информационной безопасности. Международные стандарты (GDPR, ISO/IEC 27001): их применимость и адаптация для российских образовательных учреждений. Антитеррористическая защищенность объектов в части ИТ-инфраструктуры. Регулирование оборота криптографических средств. Процедура аттестации объектов информатизации.		
Раздел 2. Управление системой защиты информации и формирование культуры информационной безопасности	4	8
Тема 3. Проектирование и эксплуатация системы технической защиты информации Моделирование угроз и определение модели нарушителя. Проектирование эшелонированной обороны (Defense in Depth). Средства сетевой безопасности. Межсетевые экраны нового поколения (NGFW). Системы обнаружения и предотвращения вторжений (IDS/IPS). Системы защиты веб-приложений (WAF). Обеспечение безопасности официальных сайтов и электронных дневников. Организация защищенного удаленного доступа. Изоляция критически важных сегментов инфраструктуры от пользовательских сетей. Обеспечение безопасности облачных сервисов. Физическая защита серверного оборудования. Процедуры реагирования на инциденты ИБ: создание и работа команды быстрого реагирования (CSIRT). Проведение аудита и мониторинга защищенности. Сканирование уязвимостей, тесты на проникновение. Автоматизация процессов по информационной безопасности в образовательной организации.	2	4
Тема 4. Управление человеческим фактором и развитие культуры кибербезопасности Разработка и внедрение Политики информационной безопасности. Трансляция правил поведения в цифровой среде. Реализация программ целевого обучения для участников образовательных отношений. Методология проведения учебных киберучений. Программы практических тренировок навыков распознавания угроз. Создание института "киберамбассадоров" или ответственных за ИБ в образовательной организации. Интеграция основ кибербезопасности в учебные программы: кросс-дисциплинарный подход через предметы информатика, ОБЗР, обществознание. Алгоритмы действий при обнаружении угроз в сети. Оценка эффективности обучающих программ. Метрики изменения уровня кибергигиены. Мотивация персонала к соблюдению правил ИБ. Процедуры контроля и этические нормы работы с данными. Развитие критического мышления и медиаграмотности как фундамента личной безопасности.	2	4
ИТОГО:	8²	16²

² Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Темы для самостоятельного изучения	Изучаемые вопросы	Кол-во часов	Формы самостоятельной работы	Методическое обеспечение	Формы отчетности
Тема 1. Концептуализация понятия «информационное пространство» и парадигма угроз в цифровой среде	1. Управление цифровыми репутационными рисками. 2. Экономические аспекты кибербезопасности. 3. Взаимосвязь физической и информационной безопасности.	18	Изучение литературы, подготовка доклада, подготовка презентации	Учебно-методическое обеспечение дисциплины	Доклад, презентация
Тема 2. Нормативно-правовой ландшафт и институциональные механизмы регулирования	1. Международные стандарты (GDPR, ISO/IEC 27001): их применимость и адаптация для российских образовательных учреждений. 2. Законодательство об образовании об обязанности образовательной организации по созданию безопасных условий обучения.	16	Изучение литературы, подготовка доклада, подготовка презентации	Учебно-методическое обеспечение дисциплины	Доклад, презентация
Тема 3. Проектирование и эксплуатация системы технической защиты информации	1. Проведение аудита и мониторинга защищенности. 2. Сканирование уязвимостей, тесты на проникновение. 3. Автоматизация процессов по информационной безопасности в образовательной организации.	20	Изучение литературы, подготовка доклада, подготовка презентации	Учебно-методическое обеспечение дисциплины	Доклад, презентация
Тема 4. Управление человеческим фактором и развитие культуры кибербезопасности	1. Мотивация персонала к соблюдению правил ИБ. 2. Процедуры контроля и этические нормы работы с данными. 3. Развитие критического мышления и медиаграмотности как фундамента личной безопасности.	18	Изучение литературы, подготовка доклада, подготовка презентации	Учебно-методическое обеспечение дисциплины	Доклад, презентация
		72 ³			

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

³ Реализуется в формате электронного обучения с применением дистанционных образовательных технологий.

5.1 Перечень компетенций с указанием этапов их формирования в процессе освоение образовательной программы

Код и наименование компетенции	Этапы формирования
ДПК-1. Способен обеспечивать и поддерживать доступность ресурсов учебного пространства и услуг, создание защищенной физической и психологической среды, способствующей успешной реализации образовательных целей и задач всеми участниками образовательного процесса;	1.Работа на учебных занятиях 2.Самостоятельная работа
ДПК-4. Способен осуществлять управление созданием безопасных условий обучения и воспитания, организации питания обучающихся и работников, обеспечению охраны их здоровья.	1.Работа на учебных занятиях 2.Самостоятельная работа

5.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Описание показателей	Критерии оценивания	Шкала оценивания
ДПК-1	Пороговый	1.Работа на учебных занятиях 2.Самостоятельная работа	Знает: нормы и правила комплексной безопасности образовательной организации Умеет: применять в профессиональной деятельности правовые нормы, регулирующие деятельность общеобразовательной организации, разрабатывать соответствующие локальные нормативные акты	Опрос, тестовое задание	Шкала оценивания опроса. Шкала оценивания тестового задания.
	Продвинутый	1.Работа на учебных занятиях 2.Самостоятельная работа	Знает: нормы и правила комплексной безопасности образовательной организации Умеет: применять в профессиональной деятельности правовые нормы, регулирующие деятельность общеобразовательной организации, разрабатывать соответствующие локальные нормативные акты Владеет способностью реализовать требования к комплексной безопасности, антитеррористической и противокриминальной защищенности общеобразовательной организации	Опрос, тестовое задание, доклад, презентация	Шкала оценивания опроса Шкала оценивания доклада Шкала оценивания тестового задания Шкала оценивания презентации
ДПК-4	Пороговый	1.Работа на учебных занятиях	Знает: требования к информационной образовательной	Опрос, тестовое задание	Шкала оценивания опроса.

		2.Самостоятельная работа	среде общеобразовательной организации. Умеет: обеспечивать соблюдение правил санитарно-гигиенического режима, техники безопасности и охраны труда; соблюдение условий транспортной безопасности		Шкала оценивания тестового задания.
	Продвинутый	1.Работа на учебных занятиях 2.Самостоятельная работа	Знает: требования к информационной образовательной среде общеобразовательной организации. Умеет: обеспечивать соблюдение правил санитарно-гигиенического режима, техники безопасности и охраны труда; соблюдение условий транспортной безопасности Владеет навыком обеспечения реализации требований к технологическим (аппаратным и программным), информационным и организационным ресурсам общеобразовательных организаций для развития информационной образовательной среды.	Опрос, тестовое задание, доклад, презентация	Шкала оценивания опроса Шкала оценивания доклада Шкала оценивания тестового задания Шкала оценивания презентации

Шкала оценивания опроса

Баллы	Критерии оценивания
5	Студент полно и аргументировано отвечает на вопросы опроса.
4	Студент дает ответ, но допускает 1-2 ошибки, которые сам же исправляет.
2	Студент обнаруживает знание и понимание основных положений данного задания, но излагает материал неполно и допускает неточности.
0	Студент обнаруживает незнание ответов на вопросы опроса.

Шкала оценивания доклада

Уровень оценивания	Критерии оценивания	Баллы
Доклад	Соответствие содержания теме доклада; глубина проработки материала; грамотность и полнота использования источников; грамотность речи и владение текстом доклада	10
	Соответствие содержания теме доклада; глубина проработки материала; использовано недостаточное количество источников; грамотность речи и владение текстом доклада	7

	Соответствие содержания теме доклада; не достаточная глубина проработки материала; использовано недостаточное количество источников; грамотность речи и владение текстом доклада	4
	Несоответствие содержания теме доклада; не достаточная глубина проработки материала; использовано недостаточное количество источников; недостаточное владение текстом доклада	0

Шкала оценивания презентации

Уровень оценивания	Критерии оценивания	Баллы
Презентация	Соответствие содержания теме; правильная структурированность информации; эстетичность оформления	10
	Соответствие содержания теме; правильная структурированность информации; недостаточная эстетичность в оформлении	7
	Соответствие содержания теме; отсутствует структурированность информации; недостаточная эстетичность в оформлении	4
	Несоответствие содержания теме; отсутствует структурированность информации; недостаточная эстетичность в оформлении	0

Шкала оценивания тестового задания

Критерии оценивания	Баллы
80-100% правильных ответов - «отлично»	8-10
60-80% правильных ответов - «хорошо»	5-7
30-50% правильных ответов - «удовлетворительно»	3-4
0-20 % правильных ответов - «неудовлетворительно»	1-2

5.3. Типовые контрольные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы.

Примерные вопросы для опроса:

1. Законодательство об образовании об обязанности образовательной организации по созданию безопасных условий обучения.
2. Требования к использованию отечественного ПО.
3. Правовое регулирование применения систем контент-фильтрации.
4. Ответственность должностных лиц за нарушение требований информационной безопасности.
5. Документальное обеспечение системы информационной безопасности.
6. Антитеррористическая защищенность объектов в части ИТ-инфраструктуры.
7. Регулирование оборота криптографических средств.
8. Процедура аттестации объектов информатизации.

9. План модернизации системы защиты: адаптация к новым технологическим вызовам.
10. Цифровая экосистема как объект управления и защиты.
11. Классификация угроз информационной безопасности: внешние и внутренние векторы атак, антропогенные и техногенные факторы риска.

Примерная тематика докладов:

1. Эволюция понятийного аппарата: от защиты информации к обеспечению безопасности цифрового периметра образовательной организации (*EdTech Security*).
2. Прогнозирование развития угроз: применение методов форсайта для стратегического планирования мер защиты.
3. Стандартизация терминологии: переход от устаревших ГОСТов к современным стандартам серии ISO/IEC 2700х.
4. Понятие «цифровой гигиены».
5. Международные стандарты (GDPR, ISO/IEC 27001): их применимость и адаптация для российских образовательных учреждений.
6. Резервное копирование и обеспечение отказоустойчивости: стратегии *Disaster Recovery Plan (DRP)* и *Business Continuity Planning (BCP)*.
7. Использование систем класса *SIEM (Security Information and Event Management)*: централизованный сбор и корреляция событий безопасности.
8. Контроль привилегированных пользователей (*PAM - Privileged Access Management*): минимизация рисков инсайдерских угроз.
9. Непрерывное образование руководителя: необходимость постоянного обновления знаний в области *EdTech* и кибербезопасности.
10. Трансформация роли руководителя ОО из администратора в архитектора безопасной цифровой среды.

Примерная тематика презентаций

1. Цифровая экосистема как объект управления и защиты.
2. Классификация угроз информационной безопасности: внешние и внутренние векторы атак, антропогенные и техногенные факторы риска.
3. Фишинговые атаки на административный персонал, *DDoS*-атаки на образовательные порталы, компрометация учетных записей учащихся.
4. Социальная инженерия как инструмент деструктивного воздействия.
5. Методы противодействия манипуляциям в корпоративной среде школы/вуза.
6. Угрозы утечки персональных данных (*PII*) участников образовательного процесса.
7. Концепция "нулевого доверия" (*Zero Trust Architecture*) в контексте обеспечения кибербезопасности ОО.
8. Развитие критического мышления и медиаграмотности как фундамента личной безопасности.
9. Формирование среды "доверия, но проверки" (*Trust but Verify*): психологические аспекты внедрения строгих политик.
10. Этические дилеммы в сфере ИБ: приватность vs безопасность, допустимость мониторинга активности.

Примерные тестовые задания:

1. В контексте проектирования системы безопасности образовательной организации концепция «нулевого доверия» (*Zero Trust Architecture*) подразумевает, что:

А) Доверие к пользователю или устройству определяется исключительно его физическим местоположением внутри периметра организации.

Б) Все запросы на доступ к ресурсам должны проходить строгую аутентификацию и авторизацию, независимо от того, находятся они внутри или снаружи сетевого периметра.

В) Основной упор делается на физическую охрану серверных помещений, а сетевой трафик считается априори безопасным.

Г) Система безопасности строится на доверии к системным администраторам, которые имеют неограниченный доступ ко всем сегментам сети.

2. Какая из перечисленных категорий данных участников образовательного процесса относится к специальным категориям персональных данных согласно 152-ФЗ?

А) Фамилия, имя, отчество и дата рождения.

Б) Сведения об успеваемости и посещаемости.

В) Сведения о состоянии здоровья (например, данные для организации инклюзивного образования).

Г) Номер мобильного телефона и адрес электронной почты.

3. При проведении категорирования объектов критической информационной инфраструктуры (КИИ) в образовательной организации ключевым фактором для присвоения категории является:

А) Общий бюджет организации на закупку ИТ-оборудования.

Б) Степень потенциального ущерба безопасности государства, причиняемого вследствие нарушения функционирования информационной системы.

В) Количество зарегистрированных пользователей в системе электронного дневника.

Г) Наличие у организации лицензии на образовательную деятельность.

4. Система класса SIEM (*Security Information and Event Management*) в первую очередь предназначена для:

А) Автоматического резервного копирования баз данных.

Б) Централизованного сбора, нормализации и корреляции событий безопасности от различных источников для выявления инцидентов в реальном времени.

В) Фильтрации веб-контента и блокировки доступа к нежелательным сайтам.

Г) Управления жизненным циклом учетных записей пользователей (*Identity Governance*).

5. В рамках формирования культуры кибербезопасности «институт киберамбассадоров» представляет собой:

А) Внешнюю консалтинговую компанию, нанятую для проведения разового аудита.

Б) Выделение из числа сотрудников или студентов неформальных лидеров мнений, ответственных за продвижение практик цифровой гигиены в своих коллективах.

В) Программный комплекс для мониторинга активности пользователей в социальных сетях.

Г) Должность штатного психолога, занимающегося проблемами интернет-зависимости.

6. Какой из перечисленных нормативных актов является основополагающим для определения состава и содержания мер по защите информации в государственных информационных системах (ГИС)?

А) Приказ ФСТЭК России от 18 февраля 2013 года № 21

Б) Приказ ФСТЭК России № 17

В) Постановление Правительства РФ от 1 ноября 2012 года 11 февраля 2013 года № 1119

Г) Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры (КИИ)»

7. Эшелонированная оборона (*Defense in Depth*) при построении системы технической защиты информации подразумевает:

- А) Использование одного, но самого мощного межсетевого экрана на границе сети.
- Б) Размещение всех серверов в одном защищенном помещении с максимальной физической охраной.
- В) Создание нескольких независимых уровней защиты (периметр, сеть, узел, приложение), чтобы компрометация одного из них не приводила к полному отказу всей системы.**

Г) Полную изоляцию внутренней сети образовательной организации от сети Интернет.

8. В чем заключается ключевое отличие теста на проникновение (*Penetration Test*) от сканирования уязвимостей (*Vulnerability Scan*)?

- А) Сканирование уязвимостей – это ручной процесс, а тест на проникновение – автоматизированный.
- Б) Сканирование уязвимостей выявляет потенциальные слабые места, а тест на проникновение – это попытка их реальной эксплуатации для оценки возможного ущерба.**

В) Тест на проникновение проводится только внешними хакерами, а сканирование – только штатными администраторами.

Г) Эти термины являются синонимами и обозначают один и тот же процесс.

9. Какая из перечисленных мер является наиболее эффективной для противодействия атакам типа «социальная инженерия» на уровне управления культурой безопасности?

- А) Установка самого современного антивирусного ПО на все рабочие станции.
- Б) Регулярное проведение практических тренингов и симуляций фишинговых атак для повышения осведомленности персонала.**
- В) Блокировка всех входящих электронных писем с вложениями.

Г) Внедрение строгой политики паролей с требованием менять их каждые 30 дней.

10. При разработке Плана обеспечения непрерывности бизнеса и восстановления после сбоев (*BCP/DRP*) для образовательной организации *RPO (Recovery Point Objective)* определяет:

- А) Максимально допустимое время, в течение которого информационная система может быть недоступна.
- Б) Максимально допустимый объем данных (в единицах времени), который может быть потерян в результате инцидента и не восстановлен из резервной копии.**
- В) Порядок действий ответственных лиц при обнаружении инцидента информационной безопасности.
- Г) Бюджетные средства, выделяемые на закупку оборудования для резервного копирования.

Перечень примерных вопросов к экзамену:

1. Эволюция понятийного аппарата: от защиты информации к обеспечению безопасности цифрового периметра образовательной организации (*EdTech Security*).
2. Архитектура современного информационного пространства образовательной организации.
3. Цифровая экосистема как объект управления и защиты.
4. Классификация угроз информационной безопасности: внешние и внутренние векторы атак, антропогенные и техногенные факторы риска.
5. Актуальные киберугрозы для сферы образования.
6. Фишинговые атаки на административный персонал, *DDoS*-атаки на образовательные порталы, компрометация учетных записей учащихся.
7. Социальная инженерия как инструмент деструктивного воздействия.
8. Методы противодействия манипуляциям в корпоративной среде школы/вуза.

9. Угрозы утечки персональных данных (*PII*) участников образовательного процесса.
10. Концепция "нулевого доверия" (*Zero Trust Architecture*) в контексте обеспечения кибербезопасности ОО.
11. Управление цифровыми репутационными рисками: мониторинг инфополя и нейтрализация негатива.
12. Психологическая безопасность в цифровой среде
13. Профилактика кибербуллинга, троллинга и других форм онлайн-агрессии среди обучающихся.
14. Экономические аспекты кибербезопасности: оценка потенциального ущерба от реализации рисков и обоснование инвестиций в защиту.
15. Взаимосвязь физической и информационной безопасности.
16. Федеральный закон № 152-ФЗ «О персональных данных»: ключевые требования к операторам ПДн в системе образования.
17. Нормативные акты ФСТЭК России и ФСБ России.
18. Требования по защите информации в государственных информационных системах (КИИ).
19. Законодательство об образовании об обязанности образовательной организации по созданию безопасных условий обучения.
20. Требования к использованию отечественного ПО.
21. Правовое регулирование применения систем контент-фильтрации.
22. Ответственность должностных лиц за нарушение требований информационной безопасности.
23. Документальное обеспечение системы информационной безопасности.
24. Антитеррористическая защищенность объектов в части ИТ-инфраструктуры.
25. Регулирование оборота криптографических средств.
26. Процедура аттестации объектов информатизации.
27. Моделирование угроз и определение модели нарушителя: практический подход к оценке рисков для конкретной ОО.
28. Проектирование эшелонированной обороны (*Defense in Depth*): многоуровневая архитектура защиты.
29. Средства сетевой безопасности: межсетевые экраны нового поколения (*NGFW*), системы обнаружения и предотвращения вторжений (*IDS/IPS*).
30. Системы защиты веб-приложений (*WAF*): обеспечение безопасности официальных сайтов и электронных дневников.
31. Организация защищенного удаленного доступа: технологии *VPN*, двухфакторная аутентификация (*2FA/MFA*).
32. Сегментация сети: изоляция критически важных сегментов инфраструктуры (серверы баз данных, бухгалтерия) от пользовательских сетей.
33. Обеспечение безопасности облачных сервисов: риски и меры защиты при использовании *SaaS*-решений (облачные хранилища, *LMS*).
34. Физическая защита серверного оборудования: контроль доступа в серверную комнату.
35. Процедуры реагирования на инциденты ИБ: создание и работа команды быстрого реагирования (*CSIRT*).
36. Проведение аудита и мониторинга защищенности: сканирование уязвимостей, тесты на проникновение (*Penetration Testing*).
37. Автоматизация процессов ИБ: внедрение инструментов для снижения человеческого фактора.
38. План модернизации системы защиты: адаптация к новым технологическим вызовам.

5.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

В рамках освоения дисциплины предусмотрены: устные опросы, тестовые задания, доклады, презентации.

Требования к экзамену

Формой промежуточной аттестации является экзамен. Экзамен проходит в форме устного собеседования по вопросам. Экзамен проводится по результатам выполнения всех видов учебной работы, предусмотренных рабочей программой дисциплины, при этом учитываются результаты текущего контроля успеваемости в течение семестра. Экзамен проводится устно по теоретическим вопросам экзаменационного билета.

За семестр студент может набрать максимально 100 баллов. Максимальное количество баллов, которое может набрать обучающийся в течение семестра за различные виды работ - 70 баллов. Максимальная сумма баллов, которые обучающийся может получить на экзамене – 30 баллов

Шкала оценивания экзамена

Баллы	Критерии оценивания
30-21	Студент демонстрирует сформированные и систематические знания; успешное и систематическое умение; успешное и систематическое применение навыков в соответствии с планируемыми результатами освоения дисциплины.
20 -6	Студент демонстрирует сформированные, но содержащие отдельные пробелы знания; сформированные, но содержащие отдельные пробелы умения; в целом успешное, но сопровождающееся отдельными ошибками применение навыков в соответствии с планируемыми результатами освоения дисциплины
5-0	Студент демонстрирует неполные знания; в целом успешные, но не систематические умения; в целом успешное, но не систематическое применение навыков в соответствии с планируемыми результатами освоения дисциплины.

Итоговая шкала выставления оценки по дисциплине

Итоговая оценка по дисциплине выставляется по приведенной ниже шкале. При выставлении итоговой оценки преподавателем учитывается работа студента в течение всего срока освоения дисциплины, а также баллы, полученные на промежуточной аттестации.

Баллы, полученные по текущему контролю и промежуточной аттестации	Оценка в традиционной системе
81-100	Отлично
61-80	Хорошо
41-60	Удовлетворительно
0-40	Неудовлетворительно

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Основная литература

1.Базанов, С.В. Комплексная безопасность образовательного учреждения [Электронный ресурс] / С. В. Базанов // Московский экономический журнал. — 2019. — № 12. — URL: <https://cyberleninka.ru/article/n/kompleksnaya-bezopasnost-obrazovatel'nogo-uchrezhdeniya-1>2.

2. Басыня Е. А. Сетевая информационная безопасность: учебник. — М.: Национальный исследовательский ядерный университет «МИФИ», 2023. — 224 с.
3. Киренберг А. Г. Информационная безопасность современных операционных систем: учебное пособие. — Кемерово: Кузбасский государственный технический университет имени Т. Ф. Горбачёва, 2022. — 138 с.
4. Чернова Е. В. Информационная безопасность человека: учебное пособие для вузов. — 3-е изд., перераб. и доп. — М.: Издательство Юрайт, 2024. — 327 с.

6.2. Дополнительная литература

2. Занько, Наталья Георгиевна. Безопасность жизнедеятельности [Электронный ресурс]: Учебник / Н.Г. Занько, К.Р. Малаян, О.Н. Русак; Под ред. О.Н. Русака. — 17. изд., стер. — Санкт-Петербург: Лань, 2021. — 704 с. — Режим доступа: <https://e.lanbook.com/book/167385>.

6.3. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Библиотека ГУП [Электронный ресурс]. — URL : <https://guppros.ru/ru/rubric/education/lib>
2. Научная электронная библиотека Elibrary [Электронный ресурс]. — URL : <https://www.elibrary.ru/>.
3. Научно-образовательный портал «Большая российская энциклопедия» [Электронный ресурс]. — URL : <https://bigenc.ru/>.
4. Национальная электронная библиотека [Электронный ресурс]. — URL : <https://rusneb.ru/>.
5. Университетская библиотека online [Электронный ресурс]. — URL : www.biblioclub.ru
6. Электронно-библиотечная система Znanium.com [Электронный ресурс]. — URL : <http://www.znaniy.com/>.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Методические рекомендации по организации самостоятельной работы студентов.

8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Программное обеспечение:

Лицензионное программное обеспечение:

Зарубежное: Microsoft Windows, Microsoft Office

Отечественное: Kaspersky Endpoint Security

Свободно распространяемое программное обеспечение:

Зарубежное: Google Chrome, 7-zip

Отечественное: ОМС Плеер (для воспроизведения Электронных Учебных Модулей)

Информационные справочные системы: система «КонсультантПлюс» Профессиональные базы данных: fgosvo.ru pravo.gov.ru www.edu.ru;

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения: комплект учебной мебели, доска, технические средства обучения (проектор подвесной, компьютер стационарный - моноблок).

Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой, подключенной к сети Интернет, обеспечены доступом к электронной информационно-образовательной среде Государственного университета просвещения. Персональные компьютеры с подключением к сети Интернет и обеспечением доступа к электронным

библиотекам и в электронную информационно-образовательную среду Университета. Доска.

Помещение для самостоятельной работы для инвалидов и лиц с ограниченными возможностями здоровья, оснащенное компьютерной техникой, подключенной к сети Интернет, обеспечено доступом к электронно-образовательной среде Университета, Комплект учебной мебели, персональные компьютеры с подключением к сети Интернет и обеспечением доступа к электронным библиотекам и в электронную информационно-образовательную среду Государственного университета просвещения, доска, проектор подвесной.