МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Забайкальский государственный университет»
(ФГБОУ ВО «ЗабГУ»)

Факультет естественных наук, математики и технологий
Кафедра Географии, безопасности жизнедеятельности и технологии

УТВЕРЖДАЮ:

Декан факультета

Факультет естественных наук, математики и технологий

Токарева Юлия Сергеевна

«____»_____20____ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.01.04 Безопасность в информационном пространстве
на 72 часа(ов), 2 зачетных(ые) единиц(ы)
для направления подготовки (специальности) 44.03.01 - Педагогическое образование

составлена в соответствии с ФГОС ВО, утвержденным приказом
Министерства образования и науки Российской Федерации от
«___» _____ 20____ г. №____

Профиль – Образование в области безопасности жизнедеятельности (для набора 2024)
Форма обучения: Заочная

1. Организационно-методический раздел

1.1 Цели и задачи дисциплины (модуля)

Цель изучения дисциплины:

формирование систематизированных знаний о системах и мерах обеспечения информационной безопасности государства, общества, личности и умение применять методы защиты от угроз в профессиональной сфере и повседневной деятельности.

Задачи изучения дисциплины:

- изучение нормативно-правовой базы по вопросам обеспечения информационной безопасности;
- умение применять методы защиты личности, общества, государства от угроз в сфере информационных потоков;
- формирование психологической устойчивости к негативным факторам средств массовой информации (СМИ), рекламы, Интернета;
- владение методами оказания педагогической и правовой помощи учащимся, пострадавшим от информационной агрессии, болезненной зависимости от Интернета и иных угроз;
- владение практическими навыками по применению мер защиты учащихся и воспитанников от информационной агрессии религиозных деятелей, экстремистов, мошенников, рекламы и СМИ.

1.2. Место дисциплины (модуля) в структуре ОП

Дисциплина «Безопасность в информационном пространстве» входит в обязательную часть цикла Б.1 Дисциплины (модули), модуль «Исследовательская и методическая деятельность в науке и образовании» учебного плана по направлению 44.03.01 Педагогическое образование направленность «Образование в области безопасности жизнедеятельности».

1.3. Объем дисциплины (модуля) с указанием трудоемкости всех видов учебной работы

Общая трудоемкость дисциплины (модуля) составляет 2 зачетных(ые) единиц(ы), 72 часов.

Виды занятий	Семестр 9	Всего часов
Общая трудоемкость		72
Аудиторные занятия, в т.ч.	14	14
Лекционные (ЛК)	6	6
Практические (семинарские) (ПЗ, СЗ)	8	8

Лабораторные (ЛР)	0	0
Самостоятельная работа студентов (СРС)	58	58
Форма промежуточной аттестации в семестре	Зачет	0
Курсовая работа (курсовой проект) (КР, КП)		

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы		Планируемые результаты обучения по дисциплине
Код и наименование компетенции	Индикаторы достижения компетенции, формируемые в рамках дисциплины	Дескрипторы: знания, умения, навыки и (или) опыт деятельности
УК-8	УК-8.1. Знает: научно обоснованные способы поддерживать безопасные условия жизнедеятельности в повседневной и профессиональной деятельности для сохранения природной среды и обеспечения устойчивого развития общества, виды опасных ситуаций; способы преодоления опасных и чрезвычайных ситуаций, военных конфликтов УК-8.2. Умеет: создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности; различать факторы, влекущие возникновение опасных ситуаций; предотвращать возникновение опасных ситуаций в целях сохранения природной среды и устойчивого развития общества УК-8.3. Владеет: навыками по предотвращению возникновения опасных ситуаций; способами поддержания гражданской обороны и условий по	Знать: научно обоснованные способы поддерживать безопасные условия жизнедеятельности в повседневной и профессиональной деятельности для сохранения природной среды и обеспечения устойчивого развития общества, виды опасных ситуаций; способы преодоления опасных и чрезвычайных ситуаций, военных конфликтов Уметь: создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности; различать факторы, влекущие возникновение опасных ситуаций; предотвращать возникновение опасных ситуаций в целях сохранения природной среды и устойчивого развития общества Владеть: навыками по предотвращению возникновения опасных ситуаций; способами поддержания гражданской

	минимизации последствий от чрезвычайных ситуаций	обороны и условий по минимизации последствий от чрезвычайных ситуаций

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

3.1 Структура дисциплины для заочной формы обучения

Модуль	Номер раздела	Наименование раздела	Темы раздела	Всего часов	Аудиторные занятия			СРС
					ЛК	ПЗ (СЗ)	ЛР	
1	1.1	История становления и нформационной безопасности в мире и РФ. Теория информационной безопасности. Нормативно-правовые основы информационной безопасности в РФ. Международные стандарты информационной безопасности. Государственная политика и нформационной безопасности.	1. Информационная безопасность: история становления и теоретические основы 2. Нормативно-правовое регулирование обеспечения информационной безопасности в РФ и в иностранных государствах	23	2	2	0	19
2	2.1	История создания и развития интернет	1. История создания и развития интернет технологий. Киберпространство.	25	2	3	0	20

		технологий. Киберпространство. Киберкультура. Правила цифрового поведения. Искусственный интеллект. Технологии виртуальной реальности. Профессии в кибероб ществе.	Киберкультура. Правила цифрового поведения. 2. Искусственный интеллект. Технологии виртуальной реальности. Профессии в кибероб ществе					
3	3.1	Информация как объект защиты. Защита информации. Защита от угрозы нарушения конфиденциальности. Конфиденциальная информация и её защита. Угрозы информационной безопасности. Информационные войны и информационное противоборство. Политика и модели безопасности. Безопасность компьютерных систем. Обеспечение информационной безопасности в РФ. Социальная	1.Информация как объект защиты. Защита информации. Защита от угрозы нарушения конфиденциальности. Конфиденциальная информация и её защита. 2.Угрозы информационной безопасности. Информационные войны и информационное противоборство. Политика и модели безопасности. 3.Безопасность компьютерных систем. Обеспечение информационной безопасности в РФ. Социальная инженерия	24	2	3	0	19

		инженерия						
Итого				72	6	8	0	58

3.2. Содержание разделов дисциплины

3.2.1. Лекционные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	1. Информационная безопасность: история становления и теоретические основы	История становления теории информационной безопасности. Предметная область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации.	1
	1.1	2. Нормативно-правовое регулирование обеспечения информационной безопасности в РФ и в иностранных государствах	Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации Основные положения Федерального закона РФ № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	1
2	2.1	1. История создания и развития интернет технологий. Киберпространство. Киберкультур	1960-е годы: создание децентрализованной сети, способной выжить при чрезвычайных обстоятельствах. 1980-е годы: Появление World Wide Web. 2000-е годы: развитие социальных сетей (Facebook, Twitter и другие), появление мобильных устройств с	1

		а. Правила цифрового поведения.	выходом в Интернет (смартфоны, планшенты) 2020-е годы: концепция Интернета Вещей - взаимодействие миллиардов устройств в реальном времени. Значение термина «киберпространство». Киберкультура как психолого-педагогическая проблема теории и практики образования. Правила цифрового этикета.	
	2.1	2. Искусственный интеллект. Технологии виртуальной реальности. Профессии в кибероблестве	Системы искусственного интеллекта. Предоставление структурированной информации. Анализ данных. Big Data. Введение в технологии виртуальной, дополненной и смешанной. Проблемы формирования изображения в системах виртуальной, дополненной и смешанной реальностей реальностей. Профессиональные стандарты кибер-профессий.	1
3	3.1	1.Информация как объект защиты. Защита информации. Защита от угрозы нарушения конфиденциальности. Конфиденциальная информация и её защита. 2.Угрозы информационной безопасности. Информационные войны и информационное противоборство. Политика и модели безопасности. 3.Безопасность компьютерны	Понятие об информации как объекте защиты. Уровни представления информации. Виды и формы представления информации. Информационные ресурсы. Классификация информационных ресурсов. Правовой режим информационных ресурсов. Анализ уязвимостей системы. Организационные методы защиты от НСД. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита целостности информации при хранении. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Определение и основные способы несанкционированного доступа. История возникновения информационно-психологических войн. История информационного противоборства. Система пропаганды в фашистской Германии как яркий пример информационной войны.	2

		х систем. Обеспечение информационной безопасности в РФ. Социальная инженерия	Виды информационной войны. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности. Содержания и основные понятия компьютерной безопасности. Общая характеристика принципов, методов и механизмов обеспечения компьютерной безопасности. Социальная инженерия как хакерство. Социальная инженерия как управление обществом. Социальная инженерия по К. Попперу. Социальная инженерия как технология. Социальная инженерия и коммуникативные технологии	

3.2.2. Практические занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Нормативно-правовое регулирование обеспечения информационной безопасности в РФ и в иностранных государствах	Информационная безопасность и ее место в системе национальной безопасности Российской Федерации Основные положения Федерального закона РФ № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	2
2	2.1	1.История создания и развития интернет технологий. Киберпространство. Киберкультур	Концепция Интернета Вещей	1

		а. Правила цифрового поведения.		
	2.1	2.Искусственный интеллект. Технологии виртуальной реальности. Профессии в киберобществе	Системы искусственного интеллекта. Предоставление структурированной информации. Анализ данных. Big Data.	2
3	3.1	Угрозы информационной безопасности. Информационные войны и информационное противоборство. Политика и модели безопасности. Безопасность компьютерных систем. Обеспечение информационной безопасности в РФ. Социальная инженерия	История возникновения информационно-психологических войн. История информационного противоборства. Система пропаганды в фашистской Германии как яркий пример информационной войны. Виды информационной войны. Принципы, методы и механизмы обеспечения компьютерной безопасности Социальная инженерия и ее проявление в современном мире.	3

3.2.3. Лабораторные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)

3.3. Содержание материалов, выносимых на самостоятельное изучение

Модуль	Номер раздела	Содержание материалов, выносимого на самостоятельное изучение	Виды самостоятельной деятельности	Трудоемкость (в часах)

1	1.1	Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.	- составление терминологической системы (словаря, глоссария, тезауруса по теме, проблеме); - подготовка сообщений и докладов; - анализ нормативных документов;	19
2	2.1	1960-е годы: создание децентрализованной сети, способной выжить при чрезвычайных обстоятельствах. Профессиональные стандарты кибер-профессий.	- подготовка электронных презентаций; - изготовление дидактических материалов; - работа с электронными образовательными ресурсами;	20
3	3.1	Информационные ресурсы. Классификация информационных ресурсов. Правовой режим информационных ресурсов. Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Определение и основные способы несанкционированного доступа.	- подготовка электронных презентаций; - изготовление дидактических материалов; - составление конспекта (опорный конспект, конспект-план, текстуальный конспект и т.п.);	19

4. Фонд оценочных средств для проведения текущей и промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств текущего контроля и промежуточной аттестации по итогам освоения дисциплины представлен в приложении.

Фонд оценочных средств

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Основная литература

5.1.1. Печатные издания

1. 1. Нестеров С. А. Основы информационной безопасности : учебник для вузов / Нестеров С. А. - 2-е изд., стер. - Санкт-Петербург : Лань, 2023. - 324 с

5.1.2. Издания из ЭБС

1. 1. Корабельников Сергей Маркович. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. - Москва : Юрайт, 2023. - 111 с. - (Высшее образование). - URL: https://urait.ru/bcode/519079 2. Казарин Олег Викторович. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для спо / О. В. Казарин, И. Б. Шубинский. - Москва : Юрайт, 2023. - 342 с. - (Профессиональное образование). - URL: https://urait.ru/bcode/518005 3. Внуков Андрей Анатольевич. Основы информационной безопасности: защита информации : учебное пособие для спо / А. А. Внуков. - 3-е изд. - Москва : Юрайт, 2023. - 161 с. - (Профессиональное образование). - URL: https://urait.ru/bcode/518006 4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для спо / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. - Москва : Юрайт, 2023. - 325 с. - (Профессиональное образование). - URL: https://urait.ru/bcode/512861

5.2. Дополнительная литература

5.2.1. Печатные издания

1. -

5.2.2. Издания из ЭБС

1. 1. Запечников Сергей Владимирович. Криптографические методы защиты информации : учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. - Москва : Юрайт, 2023. - 309 с. - (Высшее образование). - URL: https://urait.ru/bcode/511408 2. Чернова Елена Владимировна. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. - 3-е изд. - Москва : Юрайт, 2023. - 327 с. - (Высшее образование). - URL: https://urait.ru/bcode/531682 3. Зенков Андрей Вячеславович. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. - 2-е изд. - Москва : Юрайт, 2023. - 107 с. - (Высшее образование). - URL: https://urait.ru/bcode/530927 4. Прохорова О. В. Информационная безопасность и защита информации : учебник для спо /

Прохорова О. В. - 4-е изд., стер. - Санкт-Петербург : Лань, 2023. - 124 с. URL: https://e.lanbook.com/book/336200

5.3. Базы данных, информационно-справочные и поисковые системы

Название	Ссылка
ЭБС «Троицкий мост»	http://www.trmost.com
ЭБС «Лань»	https://e.lanbook.com/
ЭБС «Юрайт»	https://urait.ru/
ЭБС «Консультант студента»	https://www.studentlibrary.ru/

6. Перечень программного обеспечения

Программное обеспечение общего назначения: ОС Microsoft Windows, Microsoft Office, ABBYY FineReader, ESET NOD32 Smart Security Business Edition, Foxit Reader, АИБС "МегаПро".

Программное обеспечение специального назначения:

1) 1С-Битрикс: Корпоративный портал - Компания 1С: Предприятие 8. Комплект для обучения в высших и средних учебных заведениях 7-Zip ABBYY FineReader Adobe Audition Adobe Flash Adobe In Design Adobe Lightroom Adobe Photoshop

2) Система ГАРАНТ

3) СПС "Консультант Плюс"

7. Материально-техническое обеспечение дисциплины

Наименование помещений для проведения учебных занятий и для самостоятельной работы обучающихся	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебные аудитории для проведения занятий лекционного типа	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по факультету
Учебные аудитории для проведения практических занятий	
Учебные аудитории для проведения групповых и индивидуальных консультаций	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по кафедре
Учебные аудитории для текущей аттестации	

8. Методические рекомендации по организации изучения дисциплины

Лекционные занятия целесообразно проводить с использованием мультимедийных презентаций, которые содержат слайды теоретического характера (положения нормативных документов, основные понятия и определения) и практического характера (видеосюжеты в области обеспечения информационной безопасности, киберпреступлениях и т.д.).

Практические и семинарские занятия студентов планируется по принципу систематизации и углубления знаний учебного материала по разделам программы в форме подготовки отчетов письменных практических работ, содержащих различные формы деятельности обучающихся.

При самостоятельном рассмотрении теоретических вопросов следует обратить внимание на нормативно-правовые документы в области теории и практики информационной безопасности. Для более углубленного изучения дисциплины рекомендуется просматривать телевизионные передачи, интернет сайты с информацией о происшествиях в области информационной безопасности.

Разработчик/группа разработчиков:
Людмила Сергеевна Романова

Типовая программа утверждена

Согласована с выпускающей кафедрой
Заведующий кафедрой
_____ «___»_____20____г.