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 Математики и информатики

УТВЕРЖДАЮ:

Декан факультета

Факультет естественных наук, математики и технологий

Токарева Юлия Сергеевна

«____»_____20____ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.07.19 Защита информации
на 72 часа(ов), 2 зачетных(ые) единиц(ы)
для направления подготовки (специальности) 44.03.05 - Педагогическое образование (с двумя профилями подготовки)

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

Профиль – Информатика и физика (для набора 2024)
Форма обучения: Очная

1. Организационно-методический раздел

1.1 Цели и задачи дисциплины (модуля)

Цель изучения дисциплины:

Предметные: • сформировать систему понятий о технологиях защиты информации; • сформировать представление об основных принципах и подходах в теории защиты информации; • подготовить к решению типовых задач, связанных с безопасной эксплуатацией информационных ресурсов компьютеров и компьютерных сетей. Личностные: • развитие способности к логическому, аналитическому, критическому мышлению; • формирование готовности к саморазвитию; • формирование личной ответственности в принятии решений; • развитие общих способностей: общения и сотрудничества, точности и продуктивности в решении задач.

Задачи изучения дисциплины:

• освоение системы знаний теоретических основ организационно-правового обеспечения информационной безопасности, основных моделей систем и процессов обеспечения информационной безопасности; • освоение системы знаний в области теоретических основ информационной безопасности, защищенности средств вычислительной техники и автоматизированных информационных систем; • освоение системы знаний в области теоретических основ криптографии, принципов организации сетей конфиденциальной связи, аутентификации и разделенного доступа; • формирование умений использования защищенных сетевых протоколов и программ шифрования в индивидуальной и групповой проектно-исследовательской деятельности; • организация самостоятельной деятельности по анализу доступных средств информационных технологий и программных продуктов, позволяющих решать задачи в предметной области.

1.2. Место дисциплины (модуля) в структуре ОП

Б1.О.07.19

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 10	Всего часов
Общая трудоемкость		72
Аудиторные занятия, в т.ч.	32	32
Лекционные (ЛК)	0	0
Практические (семинарские) (ПЗ, СЗ)	0	0

Лабораторные (ЛР)	32	32
Самостоятельная работа студентов (СРС)	40	40
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
ПК-6	ПК-6.1. Знает основные способы защиты информации в персональных компьютерах и сетях.	Знать: Знать: особенности защиты информации в ПК, защита ПК и носителей информации, защита в средах Windows (Linux), архитектура механизмов защиты информации в сетях, правовые основы защиты информации.
ПК-6	ПК-6.2. Умеет обнаруживать скрытые процессы, создавать учетные записи и устанавливать пароли, разграничивать доступ, настраивать локальные политики безопасности.	Уметь: Уметь: защищать ПК от вредоносного ПО, устанавливать и настраивать межсетевой экран (Firewall), работать с программами-анализаторами трафика для компьютерных сетей.
ПК-6	ПК-6.3. Владеет различными навыками защиты информации	Владеть: Владеть: различными методиками диагностики ПК и серверов на наличие вредоносного ПО и скрытых процессов, методиками удаления вредоносного ПО и скрытых процессов, методами криптографии.

3. Содержание дисциплины

3.1. Разделы дисциплины и виды занятий

3.1 Структура дисциплины для очной формы обучения

Модуль	Номер раздела	Наименование раздела	Темы раздела	Всего часов	Аудиторные занятия			СРС
					ЛК	ПЗ (СЗ)	ЛР	
1	1.1	Технологии защиты информации	Предмет, задачи и структура курса «Технологии защиты информации». Информационная безопасность.	18	0	0	8	10
2	2.1	Криптография	Криптографические методы защиты информации. Электронная цифровая подпись.	18	0	0	8	10
3	3.1	Защита информации	Защита информации в персональных компьютерах. Защита информации в компьютерных сетях.	18	0	0	8	10
4	4.1	Вредоносное ПО	Различное вредоносное ПО, компьютерные вирусы, методы защиты.	18	0	0	8	10
Итого				72	0	0	32	40

3.2. Содержание разделов дисциплины

3.2.1. Лекционные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)

3.2.2. Практические занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)

3.2.3. Лабораторные занятия, содержание и объем в часах

Модуль	Номер раздела	Тема	Содержание	Трудоемкость (в часах)
1	1.1	Предмет, задачи и структура курса «Технологии защиты информации». Информационная безопасность.	Предмет, задачи и структура курса «Технологии защиты информации». Задачи и функции обеспечения информационной безопасности, защита информации. Защита информации в АСОД: предмет и объект, угрозы безопасности.	8
2	2.1	Криптографические методы защиты информации. Электронная цифровая подпись.	Симметричные и ассиметричные криптосистемы. Криптосистемы с открытым и закрытым ключом. Работа с программой gpg (получение открытого и закрытого ключей, шифровка и расшифровка сообщения) Электронная подпись. Управление ключами. Работа с программой gpg (получение электронной цифровой подписи)	8
3	3.1	Защита информации в персональных компьютерах. Защита информации в компьютерных сетях	Особенности защиты информации в ПК. Защита ПК и носителей информации. Защита в средах Windows (Linux). Компьютерные сети – построение и использование. Сервисы безопасности. Архитектура механизмов защиты информации в сетях. Защита ПК и носителей информации. Защита в средах Windows: пароли и учетные записи пользователей, локальные политики безопасности, использование сетевых ресурсов. Установка, настройка и эксплуатация межсетевого экрана (Firewall). Работа с программами-анализаторами трафика для компьютерных сетей.	8

4	4.1	Различное вредоносное ПО, компьютерные вирусы, методы защиты.	Скрытые процессы. Методы обнаружения скрытых процессов. Программное обеспечение. Rootkit. Exploit. Способы обнаружения. Компьютерные вирусы, классификация вирусов. Методы защиты: антивирусы.	8

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	Правовое определение понятия «информация». Основные характеристики и свойства информации. Правовое определение понятий: «информационные технологии», «информационные системы» и «информационно-телекоммуникационные сети». Объекты и субъекты информационных отношений. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации. Категории информации по видам доступа к ней. Ограничение доступа к информации. Защита информации. Правовое определение целей защиты информации. Правовые гарантии защиты информации. Обязанности обладателей информации по ее	Реферат Доклад Конспект	10

		защите. Функциональная модель системы защиты. Состав и назначение функциональных блоков. Анализ опыта защиты информации в АСОД. Объективная необходимость защиты информации в современных АСОД. Защита информации от несанкционированного размножения. Основные виды информации, подлежащие защите. Общий анализ проблемы защиты информации в современных АСОД. Эффективное использование систем защиты информации.		
2	2.1	Классификация криптографических методов. Шифрование с помощью аналитических преобразований. Эллиптические функции – реализация метода открытых ключей. Криптосистемы на основе эллиптических уравнений. Системы с открытым ключом. Типы криптографических услуг. Цифровые представления Эллиптическая криптография кривой. Электронные платы и код с исправлением ошибок	Реферат Доклад Конспект	10
3	3.1	Понятие доступа и монитора безопасности. Защита файловой системы Windows. Защита паролей. Защита файловой системы Windows. Общие сведения. Защита дисков	Реферат Доклад Конспект	10

		от копирования. Защита программ на жестком диске Защита программ от трассировки. Структура системы защиты от несанкционированного копирования. Методология проектирования гарантированно защищенных КС. Понятие угрозы информационной безопасности в КС. Понятие политики безопасности в компьютерных системах. Методология политики безопасности компьютерных систем. Архитектура системы программно-аппаратной защиты.		
4	4.1	Классификация вирусов. Механизмы заражения компьютерными вирусами. Методы и средства защиты от компьютерных вирусов. Дискретные и мандатные модели. Антивирусные средства. Структура антивирусной защиты предприятия. Профилактика заражения вирусами компьютерных систем.	Реферат Доклад Конспект	10

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. Грушо, А. А. Теоретические основы компьютерной безопасности [Текст] : учеб. пособие для студентов вузов, обучающихся по специальностям группы 090100 «Информационная безопасность» / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М. : Академия, 2009. - 272 с. - (Высшее проф. образование). - ISBN 978-5-7695-4242-8 : 317.90 р. Экземпляров 13 2. Организационно-правовое обеспечение информационной безопасности [Текст] : учеб. пособие для студентов вузов / под ред. А. А. Стрельцова. - М. : Академия, 2008. - 256 с. - (Высшее проф. образование). - ISBN 978-5-7695-4240-4 : 341 р., 296.20 р. Экземпляров 31.

5.1.2. Издания из ЭБС

1. 1. Нестеров, Сергей Александрович. Информационная безопасность : Учебник и практикум / Нестеров Сергей Александрович; Нестеров С.А. - М. : Издательство Юрайт, 2017. - 321. - (Университеты России). - ISBN 978-5-534-00258-4 : 123.67. https://biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7 2. Васильева, Ирина Николаевна. Криптографические методы защиты информации : Учебник и практикум / Васильева Ирина Николаевна; Васильева И.Н. - М. : Издательство Юрайт, 2017. - 349. - (Бакалавр. Академический курс). - ISBN 978-5-534-02883-6 : 132.68. https://biblio-online.ru/viewer/59BABD78-5536-4ED4-BB9D-55E2F19F80B2#page/5

5.2. Дополнительная литература

5.2.1. Печатные издания

1. 1. Куприянов, А. И. Основы защиты информации [Текст] : учеб. пособие для студентов, обучающихся по специальностям «Радиоэлектрон. Системы», «Средства радиоэлектрон. Борьбы», «Информ. системы и технологии» / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - М. : Академия, 2006. - 253 с. - (Высшее профессиональное образование). - ISBN 5-7695-2438-3 : 156.20 р., 161.70 р. Экземпляров 3 2. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учеб. пособие для студентов вузов, обучающихся по специальности «Информ. системы и технологии» / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. : С. А. Клейменова. - М. : Академия, 2006. - 330 с. - (Высшее профессиональное образование). - ISBN 5-7695-2592-4 : 183.70 р. Экземпляров 2. 3. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст]: учеб. пособие для студентов вузов, обучающихся по направлению 230100 (654600) «Информатика и вычислит. Техника» / П. Б. Хорев. - М. : Академия, 2005. - 254 с. - (Высшее профессиональное образование). - ISBN 5-7695-1839-1 : 148.50 р. Экземпляров 2.

5.2.2. Издания из ЭБС

1. 1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. М. : Издательство Юрайт, 2017. 309 с. (Серия : Бакалавр и магистр. Академический курс). ISBN 978-5-534-04732-5. https://biblio-

online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E 2. Криптографические методы защиты информации [Электронный ресурс] / Аверченков В.И. М. : ФЛИНТА, 2017. http://www.studentlibrary.ru/book/ISBN9785976529472.html

5.3. Базы данных, информационно-справочные и поисковые системы

Название	Ссылка
Электронная интернет библиотека «Техническая литература»	https://www.tehlit.ru/
Электронная библиотечная система «Университетская библиотека online»	https://biblioclub.ru/index.php?page=book_blocks&view=main_ub
Компьютерная справочная правовая система «КонсультантПлюс»	https://www.consultant.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) Git

2) GnuPG

3) WireShark

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 лабораторных занятий	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по факультету
Учебные аудитории для промежуточной аттестации	
Учебные аудитории для проведения групповых и индивидуальных консультаций	Состав оборудования и технических средств обучения указан в паспорте аудитории, закрепленной расписанием по кафедре

8. Методические рекомендации по организации изучения дисциплины

Указания для студентов по изучению учебного курса на основе рейтинговой системы обучения

При изучении курса «Технологии защиты информации» предусматриваются следующие виды работ:

1. Выполнение лабораторных работ, за выполнение на оценку отлично студент может получить 8 баллов.
2. Выполнение кратковременных самостоятельных работ в каждом модуле:
- написание конспекта – максимальное количество баллов 4;
- подготовка доклада – максимальное количество баллов 5;
- написание реферата – максимальное количество баллов 5.
3. Сдача итогового контроля в форме контрольного теста, максимальное количество баллов 12.
4. За несвоевременную сдачу задания в срок, снимаются штрафные баллы, 2 балла за каждое задание.

Таким образом, сумма по всем видам деятельности составляет 100 баллов, без учета пункта 4.

Оценки студентам выставляются следующим образом:

«Зачтено» от 55 до 100 баллов;

«Не зачтено» от 0 до 4 баллов;

Студент, набравший от 0 до 54 баллов, обязан сдать зачет по данной дисциплине в период сессии.

Самостоятельная работа проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений обучающихся;
- углубления и расширения теоретических знаний;
- развития познавательных способностей и активности обучающихся: творческой инициативы, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя без его непосредственного участия, студент имеет право получить консультацию у преподавателя.

Виды заданий для внеаудиторной самостоятельной работы:

- поиск информации на заданную тему,
- написание конспекта;
- написание реферата;
- подготовка доклада.

Контроль самостоятельной работы и оценка ее результатов организуется как:

- самоконтроль и самооценка обучающегося;
- контроль и оценка со стороны преподавателя.

Разработчик/группа разработчиков:
Елена Ивановна Холмогорова

Типовая программа утверждена

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