МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кемеровский государственный университет»
Кузбасский гуманирарно-педагогический институт
Факультет физической культуры, естествознания и природопользования

УТВЕРЖДАЮ
Декан
Рябов В.А.
«20» марта 2024 г.

Рабочая программа дисциплины

К.М.02. ДВ.01.01 Основы информационной безопасности
в профессиональной деятельности
Код, название дисциплины

Направление подготовки
20.03.01 Техносферная безопасность
Код, название направления

Направленность (профиль) подготовки
Безопасность технологических процессов и производств

Программа бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
Заочная

Год набора 2024

Новокузнецк 2024

Лист внесения изменений
в РПД К.М.02.ДВ.01.01 Основы информационной безопасности в профессиональной деятельности

Сведения об утверждении на 2024/2025 учебный год:
утверждена Ученым советом факультета физической культуры, естествознания и природопользования (протокол Ученого совета факультета **№ 6 от 20.03.2024 г**.)
для ОПОП 2024 года набора на 2024 / 2025 учебный год
по направлению подготовки 20.03.01 Техносферная безопасность, направленность (профиль) Безопасность технологических процессов и производств

Одобрена на заседании методической комиссии факультета ФКЕП
(протокол методической комиссии факультета **№ 3 от 20.03.2024 г**.)

Одобрена на заседании профилирующей/*обеспечивающей* кафедры геоэкологии и географии
(протокол **№ 5 от 19.02.2024** г.)зав. кафедрой Ю.В. Удодов

Оглавление

1 Цель дисциплины. 4

2 Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации. 5

3. Учебно-тематический план и содержание дисциплины. 5

3.1 Учебно-тематический план 5

3.2. Содержание занятий по видам учебной работы 7

4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации. 8

5 Учебно-методическое обеспечение дисциплины. 9

5.1 Учебная литература 9

5.2 Программное и информационное обеспечение освоения дисциплины. 10

5.2.1 Программное обеспечение 10

5.3.2 Современные профессиональные базы данных и информационные справочные системы 11

6 Иные сведения и (или) материалы 11

6.1.Примерные темы письменных учебных работ 11

6.2. Примерные вопросы и задания / задачи для промежуточной аттестации 13

1 Цель дисциплины.

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы бакалавриата (далее - ОПОП):

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

Содержание компетенций как планируемых результатов обучения по дисциплине см. таблицу 1.

Таблица 1 - Формируемые компетенции, индикаторы достижения, знания, умения, навыки (ЗУВ), формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции, закрепленные за дисциплиной	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
УК-2. Способен определять круг задач в рамках поставленной цели ивыбирать оптимальные способы их решения, исходя из действующихправовых норм, имеющихся ресурсов и ограничений	УК 2.3 Планирование Планирует реализацию задач в зоне своей ответственности с учетом имеющихся ресурсов и ограничений, действующих правовых норм. УК 2.4 Реализация, оценка и контроль Выполняет задачи в зоне своей ответственности в соответствии с запланированными результатами и точками контроля, при необходимости корректирует способы решения задач.	Знать: -базовые понятия информационной безопасности; классификацию угроз уязвимостей; -нормативно-правовую базу в области защиты информации; -основные понятия и методы обеспечения информационной безопасности; Уметь: -выделять объекты защищаемой информации; -формировать требования к построению безопасной системы; Владеть: -навыками применения правовых норм информационной безопасности при планировании профессиональной деятельности; -навыками учета и применения основных методов защиты информации при планировании и решении задач профессиональной деятельности

Место дисциплины. Дисциплина входит в состав коммуникативно-цифрового модуля и является дисциплиной выбора. Изучается на 3 курсе заочной формы обучения.

2 Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации.

Таблица 2 – Объем и трудоемкость дисциплины по видам учебных занятий

Общая трудоемкость и виды учебной работы по дисциплине, проводимые в разных формах	Объём часовпо формам обучения		
	ОФО	ЗФО	ОЗФО
1 Общая трудоемкость дисциплины	72		
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	24	8	8
Аудиторная работа (всего):			
в том числе:			
лекции			
практические занятия, семинары	24	8	8
практикумы			
лабораторные работы			
в интерактивной форме			
в электронной форме			
Внеаудиторная работа (всего):			
в том числе, индивидуальная работа обучающихся с преподавателем			
подготовка курсовой работы/контактная работа			
групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем)			
творческая работа (эссе)			
3 Самостоятельная работа обучающихся (всего)	48	60	64
4 Промежуточная аттестация обучающегося - зачет и объём часов, выделенный на промежуточную аттестацию:	-	4	-

Место дисциплины. Дисциплина входит в состав коммуникативно-цифрового модуля и является дисциплиной выбора. Изучается на 3 курсе заочной формы обучения.

3. Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 3 - Учебно-тематический план обучения

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)						Формытекущего контроля и промежуточной аттестации успеваемости
			ОФО			ЗФО/ОЗФО			
			Аудиторн. занятия		СРС	Аудиторн. занятия		СРС	
			лекц.	практ.		лекц.	практ.		
	1. Информация и ее свойства								
	1.1 Виды защищаемой информации	6		2	4		2	4	Тест №1
	1.2 Персональные данные	4		2	2			4	
	2. Правовая защита информации								
	2.1 Законодательные требования к информационной безопасности	4		2	2		2	2	Реферат
	2.2 Правовые последствия нарушений информационной безопасности	6		2	4			6	Тест №2
	3. Авторизация и аутентификация								
	3.1 Регламентация парольной аутентификации	6		2	4			6	
	3.2 Противодействие фишингу и социальной инженерии при атаке на информационную безопасность	6		2	4		2	4	
	3.3. Разработка системы биометрической защиты	6		2	4			6	Реферат
	4. Программно-аппаратная и криптографическая защита информации								
	4.1 Антивирусное программное обеспечение	6		2	4			6	
	4.2 Протоколы аутентификации	6		2	4			6	
	4.3 Криптографические преобразования	6		2	4			6	ИДЗ №1
	4.4 Стеганография	6		2	4			6	
	5. Инженерно-техническая защита информации								
	5.1 Препятствие и	6		2	4		2	4	ИДЗ №2

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)						Формытекущего контроля и промежуточной аттестации успеваемости
			ОФО			ЗФО/ОЗФО			
			Аудиторн. занятия		СРС	Аудиторн. занятия		СРС	
			лекц.	практ.		лекц.	практ.		
	маскировка источников информации								
	Промежуточная аттестация - зачет	4			4			4	
	Всего:	72		24	48		8	64	

3.2. Содержание занятий по видам учебной работы

Таблица 4 – Содержание дисциплины

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	Содержание практических занятий	
1	*Основы информационной безопасности*	
1.1	Виды защищаемой информации	*Виды тайн. Определение защищаемой информации на объекте. Определение источника информации, направления защиты информации. Определение объекта защиты.*
1.2	Персональные данные	*Классификация персональных данных. ФЗ О персональных данных*
2	*Правовая защита информации*	
2.1	Законодательные требования к информационной безопасности	*Определение минимальных требований к защите информации по нормативным документам. Распоряжения и требования ФСТЭК*
2.2	Правовые последствия нарушений информационной безопасности	*Решение практических задач по определению юридической ответственности и мер правовой защиты*
3	*Авторизация и аутентификация*	
3.1	Регламентация парольной аутентификации	*Алгоритмы определения сложности пароля. Оценка паролей. Составление рекомендаций по выбору способа аутентификации на предприятии*
3.2	Противодействие фишингу и социальной инженерии при атаке на информационную безопасность	*Претекстинг. Кейлогеры. «Злой двойник». Смишинг. Поддельные письма.* *Составление правил обнаружения и поведения при атаке на личные данные и на корпоративную и служебную информацию.*
3.3.	Разработка системы биометрической защиты	*Аутентификация «субъект соответствует». Статическая и динамическая биометрическая аутентификация.* *Разработка мер биометрической защиты*
4	*Программно-аппаратная и*	

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	криптографическая защита информации	
4.1	Антивирусное программное обеспечение	*Определение и классификация вредоносных программ. Технологии использования антивирусных программ*
4.2	Протоколы аутентификации	*Моделирование аутентификации через доверенный центр.*
4.3	Криптографические преобразования	*Шифры подстановки. Шифры перестановки. Комбинированные шифры*
4.4	Стеганография	*Применение методов стеганографии для скрытия информации*
5	*Инженерно-техническая защита информации*	
5.1	Препятствие и маскировка источников информации	*Составление схемы объекта. Определение времени проникновения злоумышленника. Использование методов препятствия и обнаружения для защиты источника информации*
	Промежуточная аттестация - *зачет*	

4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации.

Для положительной оценки по результатам освоения дисциплины обучающемуся необходимо выполнить все установленные виды учебной работы. Оценка результатов работы обучающегося в баллах (по видам) приведена в таблице 7.

Таблица 5 - Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам(БРС)

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы (18 недель)
Текущая учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий)	**60**	Практические работы (отчет о выполнении лабораторной работы) (12 работ).	**1 балл** - посещение 1 практического занятия и выполнение работы на 51-65% **3 балла** – посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 85,1-100%	12 - 36
		Индивидуальные работы (отчет о выполнении) (2 работы)	**За одну ИР :** **4 балла** (выполнено 50 - 52% заданий) **10 балла** (выполнено 86 - 100% заданий)	8 - 20
		Тесты (2 работы)	**За один тест:** **2 баллов** (выполнено 51 - 65% заданий) **4 балла** (выполнено 86 - 100% заданий)	4-8
		Реферат	**4 балла** (пороговое значение) **8 баллов** (максимальное значение)	8-16
Итого по текущей работе в семестре				32 - 80
Промежуточная аттестация (тест)	20 (100% /баллов	Решение задачи 1.	**5 балла** (пороговое значение) **10 баллов** (максимальное значение)	5 - 10
		Решение задачи 3.	**5 балла** (пороговое значение)	5 - 10

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы (18 недель)
	приведенной шкалы)		**10 баллов** (максимальное значение)	
Итого по промежуточной аттестации (экзамену)				(51 – 100% по приведенной шкале) 10 – 20 б.
Суммарная оценка по дисциплине:	Сумма баллов текущей и промежуточной аттестации			51 – 100 б.

5 Учебно-методическое обеспечение дисциплины.

5.1 Учебная литература

Основная учебная литература

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171 (дата обращения: 02.12.2012).
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433715 (дата обращения: 02.12.2012).

Дополнительная учебная литература

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. — Москва : Издательство Юрайт, 2019. — 349 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433610 (дата обращения: 02.12.2012).
2. Запечников, С. В. Криптографические методы защиты информации : учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433133 (дата обращения: 02.12.2012).
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/437163 (дата обращения: 02.12.2012).
4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и

магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966 (дата обращения: 02.12.2012).

5.2 Программное и информационное обеспечение освоения дисциплины.

5.2.1 Программное обеспечение

Учебные занятия по дисциплине проводятся в учебных аудиториях КГПИ ФГБОУ ВО «КемГУ».

105 Компьютерный класс. Учебная аудитория для проведения: - занятий лекционного типа; - занятий семинарского (практического) типа; - групповых и индивидуальных консультаций; - текущего контроля и промежуточной аттестации. **Специализированная (учебная) мебель:** доска меловая, столы, стулья. **Оборудование:** *стационарное* - компьютер преподавателя, компьютеры для обучающихся (11 шт.); *переносное* - проектор. **Используемое программное обеспечение:** MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), MozillaFirefox (свободно распространяемое ПО), GoogleChrome (свободно распространяемое ПО), Yandex.Browser (отечественное свободно распространяемое ПО), PascalABC.NET(свободно распространяемое ПО), AdobeReaderXI (бесплатная версия), WinDjView 2.0.2 (свободно распространяемое ПО). **Интернет с обеспечением доступа в ЭИОС.**	654041, Кемеровская область - Кузбасс, Новокузнецкий городской округ, г. Новокузнецк, ул. Кузнецова, д. 6
106 Помещение для самостоятельной работы обучающихся. **Специализированная (учебная) мебель:** столы, стулья, доска меловая. **Оборудование:** *стационарное* - компьютеры (4 шт.). **Используемое программное обеспечение:** MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО). **Интернет с обеспечением доступа в ЭИОС.**	654041, Кемеровская область - Кузбасс, Новокузнецкий городской округ, г. Новокузнецк, ул. Кузнецова, д. 6

5.3.2 Современные профессиональные базы данных и информационные справочные системы.

Перечень СПБД и ИСС по дисциплине

1. CITForum.ru - on-line библиотека свободно доступных материалов по информационным технологиям на русском языке - http://citforum.ru
2. Базы данных и аналитические публикации на портале «Университетская информационная система Россия», режим доступа: https://uisrussia.msu.ru/
3. Официальный интернет-портал правовой информации, режим доступа - pravo.gov.ru.
4. Государственная информационная система «Правосудие», режим доступа - sudrf.ru

6 Иные сведения и (или) материалы.

6.1.Примерные темы письменных учебных работ

Темы реферата

Раздел 2Законодательные требования к информационной безопасности

1. Международные стандарты в области информационной безопасности
2. ФЗ «О персональных данных»
3. Роль ФСТЭК в области защиты информации
4. Правовое регулирование государственной тайны
5. Правовое регулирование профессиональной тайны
6. Правовое регулирование коммерческой тайны
7. Ответственность за распространение вредоносного программного обеспечения
8. Требования ФСТЭК к антивирусному программному обеспечению
9. Регулирование деятельности операторов персональных данных
10. Правовое регулирование тайны личной жизни
11. Ответственность за несанкционированный доступ к государственной тайне
12. Роль ФСБ в области защиты информации
13. Регулирование защиты информации при электронном документообороте
14. Правовое регулирование несанкционированного доступа к личным данным в социальных сетях
15. Сертификация программного обеспечения

Раздел 2. Разработка системы биометрической защиты

16. Применение биометрической защиты в банковских системах
17. Перспективы применения биометрической защиты
18. Требования к хранению биометрических данных
19. Статическая биометрия как средство аутентификации
20. Способы атаки на биометрическую аутентификацию
21. Использование биометрической аутентификации в мобильных устройствах
22. Динамические способы биометрической аутентификации
23. Недостатки биометрической аутентификации

Темы индивидуального задания

Индивидуальное задание №1Криптографические преобразования

1. Текст был зашифрован методом простой замены. Проведите дешифрование текста.

2. Использован метод маршрутной перестановки. Дешифруйте шифротекст.

Вариант	Шифротекст
1	нрпотюряпятнвеьеаомароуееряргюптхсраддтгумеозоиолисеаьодпмнарядон сялнваоеябаневнкноапмбняолаиооаьгмоеыисяьчгчйзяобхглсьннаотракарво иемоатроетнвааннгыммьебчьяотлраосабовсьпзсиуамнлб
2	тнеорддмоуооыммеароактктхуплсевлиьобсноптвсонслоиапоеукпавояппод кжиосевнрелоаихдттдиивюбллпвавессуклсооидысптсраянбгопяоуеукмвеол утлпржоыгдвесонаыимсрзибккеямлплонсеаанквкаимахдлбдвоарюелвеовие лкипднайнгвщколоеетчсд
3	жепегкесавсзнквлбиоидомоибвлдтдаоуаллслебавнееоеручлилаалоделиадтн сехиывексанодоссевсяченрзбалвввзпхтйыотавааленаугсновачпкоярлседтва ркададуукваиптьрубоилвтотсливгсравуявмхниольковоаоалобрг
4	млвхлкауязслчнелнюыутрнчсдтауевоебсгоуьамурввзоссиорлгясомешсыктн мкюпимттычитбрниоомарнлрбахвлуулгвытееиееямоегюаоейечквлзснвмснс ссгсиаокувеаоеоьоьрнсжшрчыплебчсзвоиоодуасовсяьмдцблсыпгсомвчбаеа всатйтоткоеаебрнетсртамьачрсзвтьтоьаалбяжьхтжгьяаявдкаевеяуьад

Индивидуальное задание №2Препятствие и маскировка источников

информации

1. Построить схему объекта. Выделить источники защищаемой информации. Определить зоны, классифицировать их (независимые, пересекающиеся, вложенные).

2. Построить движение злоумышленника до источника. Описать возможные меры физической защиты для увеличения времени проникновения.

3. Определить систему контроля доступа и систему технической защиты. Определить стоимость системы защиты.

6.2. Примерные вопросы и задания / задачи для промежуточной аттестации

Таблица 7 - Примерные теоретические вопросы и практические задания к экзамену

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания
1. Информация и ее свойства	1. Классификация средств и способов защиты информации 2. Защищаемая информация. Объекты защиты 3. Персональные данные 4. Регламентирующие нормативные акты 5. Международные стандарты в области защиты информации	• Классифицировать защищаемую информацию • Определить объекты защиты на предприятии • Определить категорию персональных данных
2.Правовая защита информации	6. Информация ограниченного доступа. Правовые режимы обеспечения безопасности 7. Юридическая ответственность за правонарушения	• Определить юридическую ответственность за несанкционированный доступ к государственной тайне • Определить юридическую ответственность за распространение вредоносного ПО • Определить организационные меры защиты для ИСПДн отдела кадров
3. Авторизация и аутентификация	8. Виды фишинга 9. Средства противодействия брутфорсу 10. Виды аутентификации	• Определить вид атаки • Охарактеризовать правила смены пароля для рабочего места
4. Программно-аппаратная и криптографическая защита информации	11. Криптография. Криптоанализ. Криптология 12. Стеганография 13. Вредоносное программное обеспечения	• Определить правила поведения при обнаружении подозрительного файла • Зашифровать открытый текст методом перестановки • Зашифровать открытый текст методов подстановки
5. Инженерно-техническая защита информации	14. Маскировка 15. Классификация зон защиты на объекте 16. Пространственное скрытие	• Построить маршрут злоумышленника • Определить требуемые средства противодействия аудиоканалу утечки информации

Составитель (и): Штейнбрехер О.А., канд. техн. наук, доцент кафедры ИВТ

(*фамилия, инициалы и должность преподавателя (ей)*)