Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра безопасности жизнедеятельности

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы
_____ Абрамова С.В.
(подпись, расшифровка подписи)

« 11 » июня 2022 г.

РАБОЧАЯ ПРОГРАММА

Дисциплины (модуля)

Б1.В.ДВ.11.02 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Уровень высшего образования
БАКАЛАВРИАТ

Направление подготовки
20.03.01 Техносферная безопасность
(код и наименование направления подготовки)

Профиль: Безопасность жизнедеятельности в техносфере
(наименование направленности (профиля) образовательной программы)

Квалификация
бакалавр

Форма обучения
очная
заочная

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск, 2022

Рабочая программа дисциплины **«Информационная безопасность»** составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки **20.03.01 Техносферная безопасность**

код и наименование направления подготовки

Программу составил(и):

А. Ю. Соболев, доцент, кандидат педагогических наук

И.О. Фамилия, должность, ученая степень, ученое звание

подпись

Е.Н. Бояров, профессор, доктор педагогических наук, доцент

И.О. Фамилия, должность, ученая степень, ученое звание

подпись

Рабочая программа дисциплины «Информационная безопасность» утверждена на заседании кафедры безопасности жизнедеятельности **протокол № 13 « 11 » июня 2022 г.**

Заведующий кафедрой _____ Абрамова С.В. ___ _____

фамилия, инициалы

подпись

© ФГБОУ ВО «СахГУ»

1. Цель и задачи дисциплины *(модуля)*

Цель дисциплины *(модуля)* – формирование базовых знаний в области обеспечения информационной безопасности личности, общества и государства.

Задачи дисциплины *(модуля)*:

– ознакомление студентов с современными системами информационной безопасности, технологическими защиты информации, организационными мерами по информационной защите, правовыми принципами их функционирования;

– изучение возможностей использования защиты в работе с информационными ресурсами в различных областях жизнедеятельности.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина (модуль) «Информационная безопасность» относится к базовой/вариативной части блока 1 «Дисциплины (модули)» учебного плана, формируемой участниками образовательных отношений.

Пререквизиты дисциплины (модуля): Безопасность жизнедеятельности, Информатика, Ноксология.

Постреквизиты дисциплины: Управление техносферной безопасность, Организация охраны труда, Надзор и контроль в сфере безопасности.

3. Формируемые компетенции и индикаторы их достижения по дисциплине *(модулю)*

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. **знать:** – методы критического анализа и оценки современных научных достижений; основные принципы критического анализа; – методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа. УК-1.2. **уметь:** – получать новые знания на основе анализа, синтеза и других методов; собирать данные по сложным научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и решений на основе экспериментальных действий; – выявлять в процессе анализа проблематичность ситуации, определяет этапы ее разрешения с учетом вариативных контекстов; – находить, критически анализировать и выбирать информацию, необходимую для выработки стратегии действий по разрешению проблемной ситуации; – рассматривать различные варианты решения проблемной ситуации на основе системного подхода, оценивать их преимущества и риски; – грамотно, логично, аргументировано формулировать собственные суждения и оценки; предлагать стратегию действий; – определять и оценивать практические последствия реализации действий по разрешению проблемной ситуации;

		– применять методики поиска, сбора и обработки информации; – осуществлять критический анализ и синтез информации, полученной из разных источников; – предвидеть проблемную ситуацию и моделировать умения и навыки выхода из нее; – применять системный подход для решения поставленных задач. УК-1.3. **владеть:** – исследованием проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; – выявлением научных проблем и использованием адекватных методов для их решения; – демонстрированием оценочных суждений в решении проблемных профессиональных ситуаций; – методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач; – способностью выхода из проблемной ситуации в профессиональной деятельности.
ПК-5	Способен способностью ориентироваться в основных методах и системах обеспечения техносферной безопасности, обоснованно выбирать известные устройства, системы и методы защиты человека и окружающей среды от опасностей	ПК-5.1. **знать:** – опасности среды обитания и основные техносферные опасности; – методы защиты от техносферных опасностей и системы обеспечения техносферной безопасности; – методы и средства оценки опасностей, риска; – методы комплексной оценки состояния технических систем, направленных на идентификацию источников опасностей; – правила нормирования опасностей и антропогенного воздействия на окружающую природную среду; – методы, средства спасения человека от техногенных опасностей. ПК-5.2. **уметь:** – идентифицировать основные опасности среды обитания человека, оценивать риск их реализации; – выбирать методы защиты от опасностей и способы обеспечения комфортных условий жизнедеятельности; – определять зоны повышенного техногенного риска и экологического риска; – обоснованно выбирать известные устройства, системы и методы защиты человека и природной среды от опасностей; – участвовать в разработке средств спасения и организационно-технических мероприятиях по защите территорий и человека от природных и техногенных чрезвычайных ситуаций. ПК-5.3. **владеть:** – законодательными и правовыми актами в области безопасности и охраны окружающей среды, требованиями к безопасности технических регламентов;

		– способами и технологиями защиты в чрезвычайных ситуациях; – методами обеспечения безопасности среды обитания; – средствами защиты и контроля от техногенных опасностей; – навыками составления инструкций по безопасности при защите человека и природной среды от опасностей; – навыками измерения уровней опасностей на производстве и в окружающей среде, используя современную измерительную технику; – методами мониторинга полей и источников опасностей в среде обитания и методами оценки экологической ситуации.
ПК-9	Способен использовать знания по организации охраны труда, охраны окружающей среды и безопасности в чрезвычайных ситуациях на объектах экономики	ПК-9.1. **знать:** – основные понятия в области охраны труда, охраны окружающей среды, безопасности в ЧС на объектах экономике; – основы организации охраны труда, охраны окружающей среды и безопасности в ЧС; – характер воздействия вредных и опасных факторов на человека и природную среду; – классификацию ЧС; поражающие факторы опасных природных явлений, техногенных аварий и катастроф, методику расчета экономического ущерба при ЧС; – основные принципы и способы защиты производственного персонала; – правовые основы обеспечения безопасности в ЧС на объектах экономики; – основные техносферные опасности, их свойства и характеристики, характер воздействия вредных и опасных факторов на человека и природную среду, методы защиты от них; – действующую систему управления безопасностью на объектах экономики; ПК-9.2. **уметь:** – выбирать методы защиты от опасностей и способы обеспечения комфортных условий жизнедеятельности; – оценивать параметры поражающих факторов и очагов поражения при ЧС; – использовать знания по организации охраны труда, охраны окружающей среды и безопасности в чрезвычайных ситуациях на объектах экономики; – организовывать работу исполнителей по решению задач охраны труда, охраны окружающей среды, безопасности в ЧС на объектах экономики. ПК-9.3. **владеть:** – законодательными и правовыми актами в области безопасности и охраны окружающей среды, требованиями безопасности технических регламентов; – способами и технологиями защиты в чрезвычайных ситуациях на объектах экономики; – методами обеспечения безопасной среды обитания и методами оценки экологической ситуации;

		– навыком организации обучения сотрудников предприятий по охране труда, охране окружающей среды и безопасности в ЧС; – методами организации охраны труда на объектах экономики.
ПК-10	Способен использовать знание организационных основ безопасности различных производственных процессов в чрезвычайных ситуациях	ПК-10.1. **знать:** – теоретические основы обеспечения безопасности жизнедеятельности; – систему управления безопасностью в техносфере; – научные и организационные основы безопасности производственных процессов и устойчивости производств в чрезвычайных ситуациях; – специфику и механизм токсического действия вредных веществ, энергетического воздействия и комбинированного действия вредных факторов; – основные техносферные опасности, их свойства и характеристики, характер воздействия вредных и опасных факторов на человека и природную среду, методы защиты от них; ПК-10.2. **уметь:** – прогнозировать аварии и катастрофы; – идентифицировать основные опасности среды обитания человека, оценивать риск их реализации, выбирать методы защиты от опасностей и способы обеспечения комфортных условий жизнедеятельности; – пользоваться основными средствами контроля среды обитания; – использовать знание организационных основ безопасности различных производственных процессов в чрезвычайных ситуациях; ПК-10.3. **владеть:** – способами и технологиями защиты производства в чрезвычайных ситуациях; – законодательными и правовыми актами в области безопасности и охраны окружающей среды, требованиями безопасности технических регламентов
ПК-11	Способен организовывать, планировать и реализовывать работу исполнителей по решению практических задач обеспечения безопасности человека и окружающей среды	ПК-11.1. **знать:** – информацию о целях и задачах в области обеспечения безопасности человека и природной среды в техносфере; – теоретические основы обеспечения безопасности жизнедеятельности; – систему управления техносферной безопасности (управление экологической безопасностью, управление охраной труда, управление ГО и ЧС); ПК-11.2. **уметь:** – организовывать, планировать и реализовывать работу исполнителей по решению практических задач обеспечения безопасности человека и окружающей среды; – использовать способы и технологии защиты человека, производства и среды обитания в чрезвычайных ситуациях;

		ПК-11.3. **владеть:** – методами и средствами организации, планирования и реализации работы исполнителей по решению практических задач обеспечения безопасности человека и окружающей среды

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет 2 зачетных единиц (72 академических часов).

Очная форма обучения

Вид работы	Трудоемкость, акад. часов	
	4 семестр	всего
Общая трудоемкость	**72**	**72**
Контактная работа:	**40**	**40**
Лекции (Лек)	18	18
Практические занятия (ПР)	18	18
Лабораторные работы (Лаб)	–	–
Контактная работа в период теоретического обучения (КонтТО) *(проведение текущих консультаций и индивидуальная работа со студентами)*	4	4
Контактная работа в период аттестации (КонтПА)	–	–
Промежуточная аттестация (зачет, экзамен, зачет с оценкой)	зачет	–
Самостоятельная работа:	**32**	**32**
- выполнение индивидуального творческого задания (ИТЗ);	4	4
- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);	20	20
- подготовка к практическим занятиям;	6	6
- подготовка к промежуточной аттестации и т.п.)	2	2

Заочная форма обучения

Вид работы	Трудоемкость, акад. часов	
	5 семестр	всего
Общая трудоемкость	**72**	**72**
Контактная работа:	**9**	**9**
Лекции (Лек)	4	4
Практические занятия (ПР)	4	4
Лабораторные работы (Лаб)	–	–
Контактная работа в период теоретического обучения (КонтТО) *(Проведение текущих консультаций и индивидуальная работа со студентами)*	–	–
Контактная работа в период аттестации (КонтПА)	1	1
Промежуточная аттестация (зачет, экзамен, зачет с оценкой)	зачет	3
Самостоятельная работа:	**60**	**60**
- выполнение индивидуального творческого задания (ИТЗ);	4	4
- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);	30	30
- подготовка к практическим занятиям;	20	20
- подготовка к промежуточной аттестации и т.п.)	6	6

4.2. Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

Очная форма обучения

№ п/п	Раздел дисциплины/ темы	семестр	Виды учебной работы (в часах)			Формы текущего контроля успеваемости, промежуточной аттестации
			контактная		Самостоятельная работа	
			Лекции	Практические занятия		
1	Раздел 1. Информационная безопасность: содержание и структура понятия.	4	4	4	10	дискуссия, реферативный обзор
2	Раздел 2. Правовое обеспечение информационной безопасности.	4	2	2	10	устный ответ по вопросам, задания на анализ конкретной ситуации, демонстрация презентаций
3	Раздел 3. Организационное обеспечение информационной безопасности. Компьютерные преступления.	4	4	4	5	устный ответ по вопросам, задания на анализ конкретной ситуации, демонстрация презентаций
4	Раздел 4. Инженерно-технические средства обеспечения информационной безопасности. Защита от компьютерных вирусов	4	4	2	2	устный ответ по вопросам, демонстрация презентаций
5	Раздел 5. Способы защиты информации. Противодействие несанкционированному доступу к информационным ресурсам.	4	2	4	4	устный ответ по вопросам, задания на анализ конкретной ситуации, демонстрация презентаций
6	Раздел 6. Тайна как правовая категория	4	2	2	1	устный ответ по вопросам, задания на анализ конкретной ситуации, демонстрация презентаций
7	*зачёт*	4	–	–	–	*тестирование, опрос по билетам*
8	итого:	4	18	18	32	

Заочная форма обучения

№ п/п	Раздел дисциплины/ темы	семестр	Виды учебной работы (в часах)			Формы текущего контроля успеваемости, промежуточной аттестации
			контактная		Самостоятельная работа	
			Лекции	Практические занятия		
1	Раздел 1. Информационная	5	1	1	10	дискуссия, реферативный обзор

	безопасность: содержание и структура понятия.					
2	Раздел 2. Правовое обеспечение информационной безопасности.	5	1	1	10	устный ответ по вопросам, задания на анализ конкретной ситуации, демонстрация презентаций
3	Раздел 3. Организационное обеспечение информационной безопасности. Компьютерные преступления.	5	1	1	10	устный ответ по вопросам, задания на анализ конкретной ситуации, демонстрация презентаций
4	Раздел 4. Инженерно-технические средства обеспечения информационной безопасности. Защита от компьютерных вирусов	5	–	–	10	устный ответ по вопросам, демонстрация презентаций
5	Раздел 5. Способы защиты информации. Противодействие несанкционированному доступу к информационным ресурсам.	5	1	1	10	устный ответ по вопросам, задания на анализ конкретной ситуации, демонстрация презентаций
6	Раздел 6. Тайна как правовая категория	5	–	–	10	устный ответ по вопросам, задания на анализ конкретной ситуации, демонстрация презентаций
7	*зачёт*	5	–	–	–	*тестирование, опрос по билетам*
8	итого:	5	4	4	60	

4.3. Содержание разделов дисциплины

Раздел 1. Информационная безопасность: содержание и структура понятия.

Содержание и структура понятия «безопасность». Содержание и структура понятия «информационная безопасность». Содержание и структура понятия «обеспечение информационной безопасности». Содержание и структура понятия «угроза». Классификация угроз.

Раздел 2. Правовое обеспечение информационной безопасности.

Направления обеспечения безопасности. Основные статьи российского законодательства о компьютерных преступлениях. Основы правовой защиты информации. Структура законодательства России в области защиты информации. Основы правовой защиты информации.

Раздел 3. Организационное обеспечение информационной безопасности. Компьютерные преступления.

Структура законодательства России в области защиты информации. Основы организационных средств обеспечения информационной безопасности. Классификация средств и методов организационной защиты. Понятие компьютерного преступления. Причины совершения. Признаки. Классификация компьютерных преступлений. Понятие «хакер». Виды хакеров. Способы подготовки к действиям компьютерных преступников. Методы незаконного проникновения.

Раздел 4. Инженерно-технические средства обеспечения информационной безопасности. Защита от компьютерных вирусов.

Основы инженерно-технических средств обеспечения информационной безопасности. Классификация средств инженерно-технической защиты. Понятие компьютерного вируса. Классификация компьютерных вирусов. Основные этапы

жизненного цикла вирусов. Основные каналы распространения компьютерных вирусов. Методы и средства антивирусной защиты. Методы обнаружения вирусов. Антивирусные программы. Виды и структура. Основные критерии качества антивируса. Построение системы антивирусной защиты корпоративной сети.

Раздел 5. Способы защиты информации. Противодействие несанкционированному доступу к информационным ресурсам.

Физические средства защиты информации. Аппаратные средства защиты информации. Программные средства защиты информации. Сферы программной защиты. Средства защиты данных и программ. Криптографические средства защиты. Общая технология шифрования.

Раздел 6. Тайна как правовая категория.

Понятие конфиденциальной информации. Виды конфиденциальной информации. Коммерческая тайна. Формы защиты коммерческой тайны.

4.4. Темы и планы практических/лабораторных занятий

Практическое занятие (в форме семинара) 1 (4 ч.) Тема «Содержание основных понятий информационной безопасности»

Вопросы для обсуждения:

1. Содержание и структура понятия «безопасность».
2. Содержание и структура понятия «информационная безопасность».
3. Содержание и структура понятия «угроза».

Практическое занятие (в форме самостоятельной работы) 2 (2 ч.) Тема «Правовое обеспечение информационной безопасности»

На основе анализа Доктрины информационной безопасности РФ (2016 г.) выявить и сформулировать ключевые направления обеспечения безопасности в области информационной безопасности.

Практическое занятие (в форме семинара) 3 (2 ч.) Тема «Организационное обеспечение информационной безопасности»

Вопросы для обсуждения:

1. Понятие конфиденциальной информации.
2. Виды конфиденциальной информации.
3. Основы организационных средств обеспечения информационной безопасности.

Практическое занятие (в форме коллективной работы) 4 (2 ч.) Тема «Инженерно-технические средства обеспечения информационной безопасности»

Ознакомление с правилами работы антивирусных программ. Установка паролей на ПК.

Практическое занятие (в форме семинара) 5 (2 ч.) Тема «Способы защиты информации»

Вопросы для обсуждения:

1. Физические средства защиты информации.
2. Аппаратные средства защиты информации.
3. Программные средства защиты информации

Практическое занятие (в форме самостоятельной работы) 6 (2 ч.) Тема «Противодействие несанкционированному доступу к информационным ресурсам»

На основе работы с раздаточным материалом, предоставляемым преподавателем, составить примерный план-схему мероприятий по защите информации в организации.

Практическое занятие (в форме семинара) 7 (2 ч.) Тема «Защита от компьютерных вирусов»

Вопросы для обсуждения:

1. Классификация компьютерных вирусов.
2. Методы обнаружения вирусов.
3. Основные критерии качества антивируса.

4.5. Примерная тематика курсовых проектов (курсовых работ)

Не предусмотрено

5. Темы дисциплины (модуля) для самостоятельного изучения

Не предусмотрено

6. Образовательные технологии

Используются формы и методы обучения: индивидуальные, групповые, фронтальные, коллективные, парные со сменным составом студентов формы обучения.

Для развития творческих индивидуальных способностей студентов, повышения качества усвоения учебного материала используем следующие активные методы обучения: метод гипотез, метод прогнозирования метод придумывания, метод «Если бы…».

Использование перспективных форм учебной деятельности также нашли свое применение, это – метод «Мозгового штурма». Активно используются лекционные и семинарские занятия с использованием блоков-схем, опорных конспектов, проекционной техники, презентации.

Также широко применяются компьютерные симуляции, разбор конкретных ситуаций, в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

Дистанционное обучение с использованием ЭИОС на платформе Moodle:

– технология мультимедиа в режиме диалога;

– технология неконтактного информационного взаимодействия (виртуальные кабинеты, лаборатории);

– гипертекстовая технология (электронные учебники, справочники, словари, энциклопедии).

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1.	Информационная безопасность: содержание и структура понятия.	Лекция 1.	Вводная лекция с использованием видеоматериалов
		Семинар 1.	Презентации с использованием различных вспомогательных средств: доски, слайдов. **Круглый стол** с обсуждением проблемных вопросов, раскрывающих систему обеспечения информационной безопасности России, Доктрины информационной безопасности Российской Федерации,
		Самостоятельная работа	Консультирование и проверка домашних заданий посредством электронной почты
2.	Правовое обеспечение информационной безопасности.	Лекция 0.	**Лекция проблемная** (2 ч.) – раскрытие общих принципов законодательства Российской Федерации в области информационной безопасности с использованием видеоматериалов
		Семинар 2.	**Развернутая дискуссия (беседа)** с обсуждением доклада. Презентации с использованием различных вспомогательных средств: доски, слайдов. Показ и обсуждение подготовленных докладов. **Работа в малых группах. Вопросы для обсуждения:** Структурные компоненты системы обеспечения информационной безопасности: цели и задачи, принципы, основные факторы, главные направления, институты (органы), ресурсы, формы, средства и методы (процедуры).

			Основные задачи информационной безопасности в рамках страны, общества, государства и личности. Сферы национальных интересов РФ в области информационной безопасности и защиты информации.
		Самостоятельная работа	Консультирование и проверка домашних заданий посредством электронной почты
3.	Организационное обеспечение информационной безопасности. Компьютерные преступления.	Лекция 2.	Лекция с использованием видеоматериалов
		Семинар 3.	**Круглый стол** (встреча с представителями российских компаний, государственных и общественных организаций, мастерклассы экспертов и специалистов). **Работа в группах по заданию:** 1. Выявить структуру обеспечения информационной безопасности на предприятии. 2. Определить, главные направления обеспечения информационной безопасности. 3. Классификацию методов и средств организационной защиты информации
		Самостоятельная работа	Консультирование и проверка домашних заданий посредством электронной почты
4.	Инженерно-технические средства обеспечения информационной безопасности. Защита от компьютерных вирусов	Лекция 3.	Лекция с использованием видеоматериалов
		Семинар 4.	Дискуссия. Демонстрация презентаций с использованием различных вспомогательных средств: доски, слайдов.
		Самостоятельная работа	Консультирование и проверка домашних заданий посредством электронной почты
5.	Способы защиты информации. Противодействие несанкционированному доступу к информационным ресурсам.	Лекция 4.	Лекция с использованием видеоматериалов
		Семинар 5.	Дискуссия. Демонстрация презентаций с использованием различных вспомогательных средств: доски, слайдов
		Самостоятельная работа	Консультирование и проверка домашних заданий посредством электронной почты
6.	Тайна как правовая категория	Лекция 0.	Лекция с использованием видеоматериалов
		Семинар 6.	Развернутая беседа с обсуждением доклада.
		Самостоятельная работа	Консультирование и проверка домашних заданий посредством электронной почты

7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине *(модулю)*

Средства (фонд оценочных средств) оценки текущей успеваемости и промежуточной аттестации студентов по итогам освоения дисциплины «Безопасность жизнедеятельности» представляют собой комплект контролирующих материалов следующих видов:

- Практические занятия. Самостоятельная практическая работа студентов, направленная на углубление и закрепление теоретических знаний по соответствующим разделам дисциплины представлена ситуационными задачами, вопросами для дискуссий и т.п.
- Вопросы к самостоятельной работе. Представляют собой перечень вопросов.

Проверяется знание теоретического лекционного материала, тем, вынесенных на самостоятельную проработку, знание и понимание методик, владения практическими навыками.

- Вопросы к экзамену. Состоят из теоретических вопросов по всем разделам, изучаемым в данном семестре.

Разработанные контролирующие материалы позволяют оценить степень усвоения теоретических и практических знаний, приобретенные умения и владение опытом на репродуктивном уровне, когнитивные умения на продуктивном уровне, и способствуют формированию профессиональных и общекультурных компетенций студентов.

Перечень вопросов к зачету

1. Содержание и структура понятий «информационная безопасность», «система защиты информации», «система безопасности».
2. Угрозы конфиденциальной информации. Классификация.
3. Действия, приводящие к незаконному овладению информацией.
4. Направления обеспечения информационной безопасности.
5. Направление обеспечения информационной безопасности: правовая защита.
6. Структура законодательства РФ в области защиты информации.
7. Конфиденциальная информация.
8. Коммерческая и служебная тайна. Правовые формы защиты информации.
9. Правовые нормы обеспечения безопасности в организации.
10. Направление обеспечения информационной безопасности: организационная защита.
11. Служба безопасности организации.
12. Направление обеспечения информационной безопасности: инженерно-техническая защита.
13. Физические средства защиты информации.
14. Охранные системы, охранное телевидение, охранное телевидение.
15. Системы контроля доступа.
16. Аппаратные средства защиты.
17. Программные средства защиты.
18. Программная защита информации от несанкционированного доступа.
19. Программная защита информации от копирования.
20. Программная защита информации от разрушения.
21. Криптография и шифрование.
22. Модель классической (симметричной) криптографической системы.
23. Модель криптографической системы с открытым ключом (асимметричной).
24. Основные современные методы шифрования (один метод раскрыть подробно).
25. Способы защиты информации.
26. Организационные мероприятия по использованию технических средств защиты информации.
27. Организационно-технические мероприятия по использованию технических средств защиты информации.
28. Технические мероприятия по использованию технических средств защиты информации.
29. Разглашение конфиденциальной информации.
30. Способы пресечения разглашения.
31. Утечка информации по техническим каналам.
32. Каналы утечки информации.
33. Защита информации от утечки по визуально-оптическим каналам.
34. Защита информации от утечки по акустическим каналам.
35. Защита информации от утечки по электромагнитным каналам.
36. Защита информации от утечки по материально-вещественным каналам.
37. Несанкционированный доступ (НСД) к источникам конфиденциальной информации. Способы НСД.

38. НСД: защита от наблюдения и фотографирования.
39. НСД: противодействие подслушиванию посредством микрофонных систем.
40. НСД: противодействие радиосистемам акустического подслушивания.
41. НСД: обеспечение безопасности телефонных переговоров.
42. НСД: противодействие лазерному подслушиванию.
43. НСД: защита от незаконного подключения.
44. НСД: защита от перехвата.
45. Понятие компьютерного вируса: исторический аспект.
46. Классификация компьютерных вирусов.
47. Основные этапы жизненного цикла вирусов.
48. Основные каналы распространения компьютерных вирусов.
49. Методы и средства антивирусной защиты.
50. Методы обнаружения вирусов.
51. Антивирусные программы. Виды и структура.
52. Основные критерии качества антивируса.
53. Построение системы антивирусной защиты корпоративной сети.
54. Понятие компьютерного преступления. Причины совершения. Признаки.
55. Классификация компьютерных преступлений.
56. Понятие «хакер». Виды хакеров, исторический аспект.
57. Способы подготовки к действиям компьютерных преступников.
58. Методы незаконного проникновения.
59. Особенности раскрытия компьютерных преступлений.
60. Предупреждение компьютерных преступлений

Перечень дискуссионных тем круглого стола

1. Информация как средство отражения окружающего мира и как средство его познания. Количественные оценки и показатели качества информации.
2. Эволюция информационных процессов в обществе.
3. Информатизация и компьютеризация.
4. Информационные продукты, ресурсы и услуги.
5. Объективная необходимость и общественная потребность защиты информации.
6. Информационная безопасность личности, общества и государства.
7. Массовая и конфиденциальная информация.
8. Виды тайн.
9. Информационная безопасность как составляющая национальной безопасности. Задачи государства в этой области.
10. Информационное оружие, информационные войны и терроризм.
11. Государственные органы РФ, реализующие функции обеспечения информационной безопасности.
12. Компьютерная система как объект защиты информации.
13. Угрозы информационной безопасности в КС. Классификация угроз.
14. Общая характеристика случайных угроз информационной безопасности в компьютерных системах (КС).
15. Общая характеристика преднамеренных угроз информационной безопасности в КС.
16. Эволюция концепции информационной безопасности в КС. Основные принципы обеспечения информационной безопасности в КС.
17. Политика информационной безопасности в мире, России.
18. Реализация угроз информационной безопасности в КС путем несанкционированного доступа. Классификация каналов НСД.
19. Классификация каналов НСД. Собирательный образ потенциального нарушителя.
20. Обобщенные модели системы защиты информации в КС.
21. Одноуровневые, многоуровневые и многозвенные модели.
22. Помехоустойчивое кодирование.

23. Избыточные коды для обнаружения и исправления случайных ошибок в работу КС.

24. Контроль целостности программ и данных в процессе эксплуатации КС.

25. Аналитические методы шифрования.

Образец тестового задания

Вариант № 1

1. Свойства информации в форме сообщения:
   a. идеальность;
   b. субъективность;
   c. информационная неуничтожаемость;
   d. динамичность;
   e. материальность.
2. Свойства информации в виде сведений:
   a. материальность;
   b. измеримость;
   c. сложность;
   d. проблемная ориентированность;
   e. накапливаемость.
3. Информационная сфера – это… (свободный ответ)
4. Классификация национальных интересов:
   a. интересы – …
   b. интересы – …
   c. интересы – …
5. Информация – наиболее ценный …… современного общества (вставь пропущенное слово).
6. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков:
   a. документы;
   b. персонал;
   c. организационные единицы;
   d. промышленные образцы;
   e. научный инструментарий.
7. Поставьте в порядке важности национальные интересы:
8. Допишите различные подходы к понятию информации:
   a.
   b.
   c.
9. Составляющие национальной безопасности:
   a.
   b.
   c.
   d.
   e.
   f.
   g.
   h.
10. Общие методы обеспечения национальной безопасности:
    a.
    b.
    c.
11. Основные объекты воздействия в информационной войне:
    a.
    b.
    c.
    d.

e.

12. Перечислите информационное оружие (свободный ответ).
13. Война, есть продолжение …… другими, насильственными средствами (вставь пропущенное слово).
14. В Концепции национальной безопасности введено понятие национальных интересов, как совокупности сбалансированных интересов …… , …… , …… (вставь пропущенное слово).
15. Назовите шифр, при котором шифровку получают, находя символ в матрице букв шифрограммы на пересечении столбца с буквой открытого текста и строки с соответствующей буквой ключа:
    a. атбаш;
    b. цезаря;
    c. квадрат Полибия;
    d. аффинные криптосистемы;
    e. таблица Виженера.
16. Метод, при котором запись открытого текста и последующее считывание производится по разным путям внутри некоторой геометрической фигуры (например квадрата):
    a. метод аналитического преобразования;
    b. аддитивный метод;
    c. метод подстановки;
    d. метод перестановок.

8. Система оценивания планируемых результатов обучения

Оценка индивидуальной деятельности студентов по дисциплине складывается из следующих видов работ: 1) прослушивание лекций; 2) самостоятельная работа на практических занятиях; 3) самостоятельная внеаудиторная работа; 4) тестирование; 5) беседа на зачете.

Форма контроля	**За одну работу**		**Всего**
	миним. баллов	**макс. баллов**	
Текущий контроль:			
- учет посещения занятий	0	1	18 баллов
- опрос на лекции	1	2	67 баллов
- участие в дискуссии на семинаре	1	2	
- тестирование (разделы 1-2)	1	5	
- доклад (разделы 3-5)	1	5	
- контрольная работа (разделы 6-8)	1	5	
Промежуточная аттестация (зачет)	1	15	15 баллов
Итого за семестр (дисциплину)	41	100	100 баллов

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература

1. Информационная безопасность : учебное пособие / составители Е.Р. Кирколуп [и др.]. — Барнаул : АлтГПУ, 2017. — 316 с. — ISBN 978-5-88210-898-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/112164.

2. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров. — 4-е изд., стер. — Санкт-Петербург : Лань, 2018. — 324 с. — ISBN 978-5-8114-2290-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103908.

3. 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://urait.ru/bcode/432966.

4. Программно-аппаратные средства защиты информации : учебное пособие / Л.Х. Мифтахова, А.Р. Касимова, В.Н. Красильников [и др.]. — Санкт-Петербург : Интермедия, 2018. — 408 с. — ISBN 978-5-4383-0157-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103200.

5. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А.Е. Фаронов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 154 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100296.

9.2. Дополнительная литература

1. Галатенко В.А. Основы информационной безопасности: Курс лекций. – М.: Интернет- Университет Информационных технологий, 2003. – 239 с.

2. Мамаев М. Технологии защиты информации в Интернете / М. Мамаев, С. Петренко. – СПб.: ПИТЕР, 2002 . – 848 с.

3. Партыка Т. Л. Информационная безопасность : учеб. пособие для студ. учр. сред. проф. образования, обуч. по спец. информатики и выч. техники / Т. Л. Партыка, И. И. Попов. – М.: Форум: ИНФРА-М, 2005. – 368 с.

4. Рассолов, И. М. Информационное право : учебник и практикум для академического бакалавриата / И. М. Рассолов. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 347 с. — (Бакалавр. Специалист. Магистр). — ISBN 978-5-534-04348-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/431833.

5. Шульц, В. Л. Безопасность предпринимательской деятельности : учебник для вузов / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко ; под редакцией В. Л. Шульца. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 585 с. — (Высшее образование). — ISBN 978-5-534-12368-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/447405.

6. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285.

9.3. Периодические издания

Журнал «Безопасность информационных технологий». ISSN 2074-7128

Журнал «Информация и безопасность». ISSN 1682-7813

9.4. Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsift Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Proffesional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная),

(лицензия 60939880),

9. Microsoft Windows 10 Pro, 64 bit, Rus, OEM, Операционная система

10. Неисключительное право на использование ПО Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition.

11. Неисключительное право на использование ПО Kaspersky Security для виртуальных и облачных сред, Server, VirtSvr, License, Education Renewal

12. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),

13. Microsoft Volume Licensing Service, (бессрочная), (лицензия 62824441),

14. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014

15. Visual Studio Professional

16. «Антиплагиат. ВУЗ». Лицензионный договор № 5044 от 14.05. 2022 года (ежегодное продление)

9.5. Профессиональные базы данных и информационные справочные системы современных информационных технологий *(обязательно!)*

Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)

Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)

ЭБС IPRBooks Режим доступа: http://www.iprbookshop.ru

ЭБС издательства «Юрайт» Режим доступа: http://biblio-online.ru

Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru/

Ресурсы издательства Elsevier Режим доступа: http://www.sciencedirect.com

Федеральный портал «Российское образование» Режим доступа: www.edu.ru

Словари и энциклопедии на Академике. Режим доступа: http://dic.academic.ru/

Сайт Библиотеки по естественным наукам Российской академии наук. Режим доступа: http://www.benran.ru

Сайт Госкомстата РФ. Режим доступа: http://www.gks.ru

Сайт Российской государственной библиотеки. Режим доступа: http://diss.rsl.ru

Базы данных по законодательству Российской Федерации. Режим доступа: http://ru.spinform.ru

10. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

– письменные задания оформляются увеличенным шрифтом;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

Для глухих и слабослышащих:

– лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

– письменные задания выполняются на компьютере в письменной форме;

– экзамен и зачёт проводятся в письменной форме на компьютере; возможно

проведение в форме тестирования.

Для лиц с нарушениями опорно-двигательного аппарата:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

– в печатной форме увеличенным шрифтом;

– в форме электронного документа;

– в форме аудиофайла.

Для глухих и слабослышащих:

– в печатной форме;

– в форме электронного документа.

Для обучающихся с нарушениями опорно-двигательного аппарата:

– в печатной форме;

– в форме электронного документа;

– в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

Для слепых и слабовидящих:

для глухих и слабослышащих:

– автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;

– акустический усилитель и колонки;

Для обучающихся с нарушениями опорно-двигательного аппарата:

– передвижными, регулируемыми эргономическими партами СИ-1;

– компьютерной техникой со специальным программным обеспечением.

11. Материально-техническое обеспечение дисциплины (модуля)

1. Специализированные аудитории с наличием мультимедийного комплекса (компьютерная техника, мультимедийный проектор, экран, видео-, аудиоаппаратура).
2. Аудитории с наличием тематических стендов и технической аппаратуры.

Для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы используются учебные аудитории, отвечающие противопожарным правилам и нормам, обеспечивающих проведение всех видов деятельности обучающихся при освоении дисциплины, а также помещения для хранения и профилактического обслуживания учебного оборудования.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения (мультимедийными комплексами), служащими для представления учебной информации большой аудитории.

В целом, для проведения лекционных занятий: лекционные учебные аудитории материально-техническое оснащение которых составляют: учебно-наглядные пособия: наглядно-дидактические материалы. Столы аудиторные, стол преподавательский, стулья аудиторные, стул преподавательский, кафедра, доска микшер, микрофон, аудио-видео усилитель , ноутбук, Операционная система Microsoft Windows 10, Microsoft Office Professional Plus 2007.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети «Интернет» и обеспечены доступом в электронную информационно-образовательную среду вуза.

К рабочей программе прилагаются:

Приложение 1 – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю) (*разрабатывается в виде отдельного документа);*

Приложение 2 - Методические указания для обучающихся по освоению дисциплины (модуля).

(Методические указания для обучающихся по освоению дисциплины (модуля) могут быть представлены в виде изданных печатным и (или) электронным способом методических разработок со ссылкой на адрес электронного ресурса в виде рекомендаций обучающимся по изучению разделов и тем дисциплины (модуля) указанием глав, разделов, параграфов, задач, заданий, тестов и т.п. из рекомендованного списка литературы.)

УТВЕРЖДЕНО
Протокол заседания кафедры
№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

(Изменения и дополнения в РПД вносятся ежегодно и оформляются в данной форме. Изменения вносятся заменой отдельных листов (старый лист при этом цветным маркером перечеркивается, а новый лист с изменением степлером прикалывается к рабочей программе (хранится на кафедре), в электронной форме РПД должна быть актуализированной всегда, т.е. с внесенными изменениями.

При наличии большого количества изменений и поправок, затрудняющих понимание, возникших в связи с изменением нормативной базы ВО и другим причинам, проводится полный пересмотр РПД (т.е. выпускается новая РПД), которая проходит все стадии проверки и утверждения).

в рабочей программе *(модуле)* дисциплины_____
(название дисциплины)
по направлению подготовки *(специальности)*_____

на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель подпись расшифровка подписи
дата

Зав. кафедрой подпись расшифровка подписи