МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
филиала ФГБОУ ВО ВВГУ в г. Уссурийске

Рабочая программа дисциплины (модуля)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление и направленность (профиль)
44.03.05 Педагогическое образование (с двумя профилями подготовки).
Информатика и математика

Год набора на ОПОП
2023

Форма обучения
очная

Уссурийск 2023

Рабочая программа дисциплины (модуля) «Информационная безопасность» составлена в соответствии с требованиями ФГОС ВО по специальности 44.03.05 Педагогическое образование (с двумя профилями подготовки) (утв. приказом Минобрнауки России от 22.02.2018г. №125) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 N 245).

Составитель(и):
Комашинская Т.С., кандидат физико-математических наук, доцент

Утверждена на заседании Педагогического совета от 04.07.2023, протокол № 21.

СОГЛАСОВАНО:

Заместитель директора _____ Улитина О.А.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целями освоения дисциплины «Информационная безопасность» является формирование у студентов комплекса знаний, навыков и компетенций в области информационной безопасности и применения на практике методов и средств защиты информации.

Основными задачами изучения дисциплины являются:

- сформировать у студентов знания о современных тенденциях угроз информационной безопасности, о нормативных правовых документах по защите информации;
- сформировать у студентов устойчивое понимание роли и значения информационной безопасности личности, общества и государства и информационной инфраструктуры общества и государства;
- сформировать у студентов общие представления о современных методах и средствах защиты информации.

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
44.03.05 «Педагогическое образование» (с двумя профилями подготовки) (Б-ПО)	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.3п Анализирует источники информации с целью выявления их противоречий и поиска достоверных суждений	РД1	Знание	основные задачи информационной безопасности, методы и средства и технологии их решения
			РД2	Умение	оценить защищенность и обеспечение информационной безопасности объектов информатизации
			РД3	Навыки	способностью использовать для решения задач обеспечения информационной безопасности современные технические средства и информационные технологии.

	ПКР-2 Способен осуществлять целенаправленную воспитательную деятельность	ПКР-2.1п Демонстрирует умение постановки воспитательных целей, проектирования воспитательной деятельности и методов ее реализации в соответствии с требованиями ФГОС ОО и спецификой учебного предмета	РД4	Умение	проектирования воспитательной деятельности в том числе с обеспечением требований нормативных документов
	ПКР-3 Способен формировать развивающую образовательную среду для достижения личностных, предметных и метапредметных результатов обучения средствами преподаваемых учебных предметов	ПКР-3.1п Владеет способами интеграции учебных предметов для организации развивающей учебной деятельности (исследовательской, проектной, групповой и др.)	РД5	Навыки	применять на практике основные принципы теории информационной безопасности

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Информационная безопасность» специальности 44.03.05 Педагогическое образование (с двумя профилями подготовки) и изучается в 9 семестре.

Знания и умения, полученные при изучении дисциплины, необходимы обучающимся для освоения предметных компетенций и решения задач межличностного, межкультурного и профессионального взаимодействия.

Понятийный, методологический и технологический материал курса играет важную роль в формировании научного мировоззрения будущего учителя информатики и математики, его информационной грамотности.

3 Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обучения	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудоемкость	Объем контактной работы (час)						СРС	Форма аттестации
				(З.Е.)	Всего	Аудиторная			Внеаудиторная			
						лек.	прак.	лаб.	ПА	КСР		

44.03.05 «Педагогическое образование» (с двумя профилями подготовки)	ОФО	Б.1.Б.П1.07	9	4	61	20	40	0	1	0	83	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля)

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Задачи информационной безопасности	РД1, РД2	4	10	0	20	Опрос Тест
2	Понятие и виды защищаемой информации	РД3, РД4	6	10	0	20	Опрос
3	Криптографические методы защиты информации	РД2	4	10	0	20	Опрос
4	Программноаппаратные средства защиты информации	РД5	6	10	0	23	Опрос
Итого по таблице			**20**	**40**	**0**	**83**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОЗФО

Тема 1 Задачи информационной безопасности.

Содержание темы:

Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженернотехническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде. Задача обеспечения конфиденциальности. Задача обеспечения аутентификации. Обеспечение идентификации. Задача обеспечения целостности.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: кооперативное обучение, проблемный метод и метод проектов; технология учебной дискуссии, технология дидактической игры.

Виды самостоятельной подготовки студентов по теме: проработать и законспектировать рекомендуемую литературу; подготовить доклады и сообщения по вопросам темы.

Тема 2 Понятие и виды защищаемой информации.

Содержание темы: Классификация угроз информационной безопасности. Угрозы несанкционированного доступа к данным. Угрозы нарушения целостности данных. Угрозы нарушения конфиденциальности данных. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: кооперативное обучение, проблемный метод и метод проектов; технология учебной дискуссии, технология дидактической игры.

Виды самостоятельной подготовки студентов по теме: проработать и законспектировать рекомендуемую литературу; подготовить доклады и сообщения по вопросам темы.

Тема 3 Криптографические методы защиты информации.

Содержание темы: Общая характеристика способов и средств защиты информации. Основные понятия криптографии. Симметричные шифры. Криптография с открытым ключом. Схемы идентификации и аутентификации. Одно- и многофакторная аутентификация. Система разграничения доступа к информации в компьютерной системе. Концепция построения систем разграничения доступа.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: кооперативное обучение, проблемный метод и метод проектов; технология учебной дискуссии, технология дидактической игры.

Виды самостоятельной подготовки студентов по теме: проработать и законспектировать рекомендуемую литературу; подготовить доклады и сообщения по вопросам темы.

Тема 4 Программноаппаратные средства защиты информации.

Содержание темы: Схемы идентификации и аутентификации. Одно- и многофакторная аутентификация. Система разграничения доступа к информации в компьютерной системе. Концепция построения систем разграничения доступа. Средства и методы ограничения доступа к файлам. Понятие о цифровой подписи. Подпись RSA. Подпись ElGamal. Подпись DSA. Аппаратные и программно-аппаратные средства криптозащиты данных. Использование дополнительных плат расширения. Методы “водяных знаков” и методы “отпечатков пальцев”. Защита программ от несанкционированного копирования. Вирусы.

Виды самостоятельной подготовки студентов по теме: проработать и законспектировать рекомендуемую литературу; подготовить доклады и сообщения по вопросам темы.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы, выполнение аттестационных мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную подготовку к практическим занятиям, выполнение творческих заданий, самостоятельное изучение некоторых разделов курса.

Практические задания выполняются студентами как аудиторно, так и самостоятельно. В начале занятия преподаватель информирует студентов о требованиях и дает рекомендации по выполнению каждой практической работы.

Работа над практическими заданиями включает: качество проделанных практических работ, посещаемость занятий, результаты самостоятельной работы по выполнению практических заданий.

Подготовке студента к выполнению работ на практическом занятии должно предшествовать изучение литературы, приведенной в списке основной и дополнительной литературы рабочей программы учебной дисциплины. При этом, желательно, чтобы студенты проводили анализ полученной дополнительной информации, анализировали существенные дополнения и ставили вопросы. В процессе самостоятельной подготовки используются электронные базы данных и различные электронные ресурсы. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Темы практических заданий, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в ФОС к дисциплине.

Текущий контроль проводится по результатам работы студентов на практических занятиях и самостоятельной работы по выполнению практических заданий. Критерием оценки является полнота выполнения практических работ, выполнение их в точном соответствии с постановкой и творческий подход к решению проблем.

Организация образовательного процесса регламентируется учебным планом и расписанием учебных занятий. Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

При формировании своей индивидуальной образовательной траектории обучающийся имеет право на переаттестацию соответствующих дисциплин (модулей), освоенных в процессе обучения, который в том числе освобождает обучающегося от необходимости их повторного освоения.

Преподавание дисциплины основано на использовании педагогических технологий, ориентированных на развитие личности студента.

Обучение в сотрудничестве. К нему относятся: кооперативное обучение, проблемный метод и метод проектов.

Используются также активные методы обучения, в числе которых:

- анализ конкретных ситуаций, предполагающий определение проблемы, ее коллективное обсуждение, позволяющее познакомить студентов с вариантами разрешения конкретной проблемной задачи;

- «круглый стол», ориентированный на выработку умений обсуждать проблемы, обосновывать предполагаемые решения и отстаивать свои убеждения.

Интерактивные методы и формы обучения:

• Работа в группах.

• Ролевая и деловая игра.

• Решение ситуационных задач.

• Учебная дискуссия.

Методические рекомендации по обеспечению самостоятельной работы

Общий объём самостоятельной работы студентов по дисциплине включает аудиторную и внеаудиторную самостоятельную работу студентов в течение семестра. Аудиторная самостоятельная работа осуществляется в форме контрольных работ на занятиях по блоку тем, внеаудиторная самостоятельная работа осуществляется в следующих формах:

- Подготовка к практическим занятиям;

- Подготовка к текущим контрольным мероприятиям (контрольные работы, тестовые опросы, диктанты);

- Выполнение домашних индивидуальных заданий;
- Другие виды работ (работа в ЭОС, работа с медиа материалами).

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. *Зенков, А. В.* Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/530927

2. *Чернова, Е. В.* Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531682

3. *Суворова, Г. М.* Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531084

7.2 Дополнительная литература

1. *Щербак, А. В.* Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519614

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511239

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости)

1. Электронная библиотечная система «РУКОНТ» - Режим доступа: https://lib.rucont.ru/
2. Электронная библиотечная система издательства "Юрайт" - Режим доступа: https://urait.ru/
3. Электронная библиотечная система «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» - Режим доступа: http://biblioclub.ru/
4. Профессиональная база данных Open Academic Journals Index - Режим доступа: http://oaji.net/
5. Всемирная энциклопедия искусства [Электронный ресурс]: artprojekt.ru. – Режим доступа: http://www.artprojekt.ru/
6. База данных Directory of Open Access Journals - Режим доступа: http://doaj.org/
7. База данных международных индексов научного цитирования Scopus - Режим доступа: https://www.scopus.com/search/form.uri?display=basic#basic
8. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:
· Компьютеры
· Проектор

Программное обеспечение:
· ABBYY Fine Reader 11 Professional Edition
· Диалог Nibelung 2.0 Russian

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации.

Рабочие места на базе компьютерной техники с возможностью подключения к информационно-телекоммуникационной сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

персональные компьютеры; посадочных мест – 18 шт. Стол преподавателя - 1 шт; Стул преподавателя - 1 шт; Доска маркерная - 1 шт.

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
филиала ФГБОУ ВО ВВГУ в г. Уссурийске

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление и направленность (профиль)
44.03.05 Педагогическое образование (с двумя профилями подготовки).
Информатика и математика

Год набора на ОПОП
2023

Форма обучения
очная

Уссурийск 2023

1 Перечень формируемых компетенций

Название ОПОП ВО	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
44.03.05 «Педагогическое образование» (с двумя профилями подготовки) (Б-ПО)	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.3п Анализирует источники информации с целью выявления их противоречий и поиска достоверных суждений
	ПКР-2 Способен осуществлять целенаправленную воспитательную деятельность	ПКР-2.1п Демонстрирует умение постановки воспитательных целей, проектирования воспитательной деятельности и методов ее реализации в соответствии с требованиями ФГОС ОО и спецификой учебного предмета
	ПКР-3 Способен формировать развивающую образовательную среду для достижения личностных, предметных и метапредметных результатов обучения средствами преподаваемых учебных предметов	ПКР-3.1п Владеет способами интеграции учебных предметов для организации развивающей учебной деятельности (исследовательской, проектной, групповой и др.)

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

Компетенция ПКР-2: Способен осуществлять целенаправленную воспитательную деятельность

Компетенция ПКР-3: Способен формировать развивающую образовательную среду для достижения личностных, предметных и метапредметных результатов обучения средствами преподаваемых учебных предметов .

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	

УК-1.3п Анализирует источники информации с целью выявления их противоречий и поиска достоверных суждений	РД1	Знание	основные задачи информационной безопасности, методы и средства и технологии их решения	Обладает фондом новых педагогических знаний о профессиональной компетентности педагога
	РД2	Умение	оценить защищенность и обеспечение информационной безопасности объектов информатизации	Способен решать стандартные профессиональные задачи с использованием существующих информационно-коммуникационных технологий
	РД3	Навыки	способностью использовать для решения задач обеспечения информационной безопасности современные технические средства и информационные технологии	Владеет методикой и техникой решения задач по элементарной математике; языком математики; культурой математического мышления
ПКР-2.1п Демонстрирует умение постановки воспитательных целей, проектирования воспитательной деятельности и методов ее реализации в соответствии с требованиями ФГОС ОО и спецификой учебного предмета	РД4	Умение	проектирования воспитательной деятельности в том числе с обеспечением требований нормативных документов	Умение проектировать воспитательную деятельность, учитывая требования нормативных документов
ПКР-3.1п Владеет способами интеграции учебных предметов для организации развивающей учебной деятельности (исследовательской, проектной, групповой и др.)	РД5	Навыки	применять на практике основные принципы теории информационной безопасности	Способен применять на практике основные принципы теории информационной безопасности

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения	Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
		Текущий контроль	Промежуточная аттестация
Очная форма обучения			

РД1	Знание : основные задачи информационной безопасности, методы и средства и технологии их решения	Задачи информационной безопасности	Опрос Тест	Собеседование
РД2	Умение : Способен решать стандартные профессиональные задачи с использованием существующих информационно-коммуникационных технологий	Задачи информационной безопасности	Опрос Тест	Собеседование
		Криптографические методы защиты информации	Опрос	Собеседование
РД3	Навыки: способностью использовать для решения задач обеспечения информационной безопасности современные технические средства и информационные технологии	Понятие и виды защищаемой информации	Опрос	Собеседование
РД4	Умение : проектирования воспитательной деятельности в том числе с обеспечением требований нормативных документов	Понятие и виды защищаемой информации	Опрос	Собеседование
РД5	Навыки: применять на практике основные принципы теории информационной безопасности	Программноаппаратные средства защиты информации	Опрос	Собеседование

4 Описание процедуры оценивания

Текущий контроль успеваемости по дисциплине осуществляется путем оценки результатов выполнения тестовых заданий, самостоятельной работы, посещения лекций и по ответам на вопросы при подготовке к практическим занятиям, собеседования, опроса.

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические работы, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» / «неудовлетворительно»	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примеры оценочных средств

5.1 Опрос

Примерный перечень вопросов

1. Определение информационной безопасности.
2. Определение безопасности компьютерной системы.
3. Какие преступления бывают в интернете?
4. Основные технологии и методы компьютерных преступлений.
5. Какие уровни информационной защиты существуют?
6. Какие существуют способы защиты информационной безопасности?

7. Что такое концепция информационной безопасности?
8. Угрозы безопасности данных.
9. Информационная война, методы и средства её ведения.
10. Информационное оружие, его классификация и возможности.
11. Избирательное управление доступом.
12. Авторизация пользователей.
13. Аутентификация с помощью биометрических характеристик.
14. Источники угроз безопасности персональных данных.

Критерии оценивания устного ответа

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

5.2 Тест

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

a) Разработка аппаратных средств обеспечения правовых данных
b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

a) Хищение жестких дисков, подключение к сети, инсайдерство

b) Перехват данных, хищение данных, изменение архитектуры системы
c) Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
a) Персональная, корпоративная, государственная
b) Клиентская, серверная, сетевая
c) Локальная, глобальная, смешанная

4) Цели информационной безопасности
a) своевременное обнаружение, предупреждение:
b) несанкционированного доступа, воздействия в сети
c) инсайдерства в организации - чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
a) Компьютерные сети, базы данных
b) Информационные системы, психологическое состояние пользователей
c) Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
a) Искажение, уменьшение объема, перекодировка информации
b) Техническое вмешательство, выведение из строя оборудования сети
c) Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
a) Экономической эффективности системы безопасности
b) Многоплатформенной реализации системы
c) Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
a) руководители, менеджеры, администраторы компаний
b) органы права, государства, бизнеса
c) сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
a) Установление регламента, аудит системы, выявление рисков
b) Установка новых офисных приложений, смена хостинг-компании
c) Внедрение аутентификации, проверки контактных данных пользователей тест

10) Принципом информационной безопасности является принцип недопущения:
a) Неоправданных ограничений при работе в сети (системе)
b) Рисков безопасности сети, системы
c) Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
a) Невозможности миновать защитные средства сети (системы)
b) Усиления основного звена сети, системы
c) Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

a) Усиления защищенности самого незащищенного звена сети (системы)
b) Перехода в безопасное состояние работы сети, системы
c) Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
a) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
b) Одноуровневой защиты сети, системы
c) Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
a) Компьютерный сбой
b) Логические закладки («мины»)
c) Аварийное отключение питания

5.3 Собеседование

Примерный перечень вопросов

Примерный перечень вопросов

1. Ценность информации. Цена информации.
2. Какие могут быть мероприятия по обеспечению информационной безопасности?
3. Методы несанкционированного доступа к информации.
4. Процедура идентификации, как основа процесса обнаружения объекта.
5. Защита личности как носителя информации.
6. Классификация вирусов.
7. Компьютерная преступность. Виды преступной деятельности.
8. Классификация антивирусных программ.
9. Какую информацию нельзя распространять?
10. Причины, виды, каналы утечки и искажения информации.

Краткие методические указания

Необходимо проработать и законспектировать рекомендуемую литературу. Подготовить сообщения по вопросам темы. Кроме того, следует подобрать из наиболее доступной литературы дополнительные сведения по вопросам обсуждения, подтверждающие основные идеи темы.

Собеседование проводится в форме дискуссии и направлено на проверку и оценивание знаний, умений и навыков полученных в ходе плановых практических занятий, а именно работать с учебной, методической и научной литературой, с информационными ресурсами, а также навыков самостоятельной работы в использовании информационных ресурсов (в том числе мультимедийных) и компьютерных технологий для обработки, передачи, систематизации информации и доклада результатов познавательной и практической деятельности.