Министерство просвещения Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ульяновский государственный педагогический университет
имени И.Н. Ульянова»
(ФГБОУ ВО «УлГПУ им. И.Н. Ульянова»)

Факультет физико-математического и технологического образования
Кафедра информатики

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0233C9D60038B01A9E48C1A3FBB4A9D9F6
Владелец: Титов Сергей Николаевич
Действителен: с 07.07.2023 до 28.04.2038

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ _____С.Н. Титов
«_____» _____ 2023 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИЛИ ЗАЩИТА ИНФОРМАЦИИ

Программа учебной дисциплины
коммуникативного модуля по направлению
38.03.03 Управление персоналом
(очно-заочное обучение)

Составитель: Сайфутдинов Р.А.,
доцент кафедры информатики

Рассмотрено и утверждено на заседании ученого совета факультета права, экономики и управления, протокол от 30 мая 2023 г. № 9

Ульяновск, 2023

1. Наименование дисциплины

Дисциплина «Информационная безопасность или защита информации» включена в часть формируемую участниками образовательных отношений дисциплины по выбору Б1.В.ДВ.2 учебного плана основной профессиональной образовательной программы высшего образования – программы по направлению подготовки 38.03.03 Управление персоналом, очно-заочной формы обучения.

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

Целью освоения дисциплины «Информационная безопасность или защита информации» является прочное и сознательное овладение студентами знаниями и умениями в области защиты информации для осуществления профессиональной деятельности

В результате освоения программы обучающийся должен овладеть следующими результатами обучения по дисциплине «Информационная безопасность или защита информации»

<table>
<tr><td rowspan="2">Компетенция и индикаторы ее достижения в дисциплине</td><td colspan="3">Образовательные результаты дисциплины
(этапы формирования дисциплины)</td></tr>
<tr><td>знает</td><td>умеет</td><td>владеет</td></tr>
<tr><td>ПК-11
Способен вести кадровое делопроизводство и организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами, владеет навыками составления кадровой отчетности, умеет обеспечить защиту персональных данных сотрудников
ПК-11.1
Знает основы архивного законодательства и нормативные правовые акты Российской Федерации, в части ведения документации по персоналу
ПК-11.2
Способен организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами
ПК-11.3
Знает технологии, методы и методики проведения анализа и систематизации документов и информации
ПК-11.4
Умеет разрабатывать проекты кадровых документов
ПК-11.5
Умеет пользоваться поисковыми системами и</td><td>ОР-1
- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- источники и классификацию угроз информационной безопасности;
- основные средства и способы защиты информации при работе на компьютере;
- правовые основы организации защиты государственной тайны и конфиденциальной информации

ОР-4
- основы современных технологий сбора, обработки и представления информации;</td><td>ОР-2
- применять правовые, организационные, технические и программные средства защиты информации;
- создавать программные средства защиты информации;
- организовывать безопасную работу в Интернет и отправку почтовых сообщений в глобальной сети;

ОР-5
- использовать современные информационно-коммуникационные технологии (включая пакеты прикладных программ, локальные и глобальные компьютерные сети) для сбора, обработки и анализа информации.</td><td>ОР-3
- способами организации защиты информации в компьютерных сетях;
- средствами защиты данных от разрушающих воздействий компьютерных вирусов;
- базовыми программными методами защиты информации при работе с компьютерными системами и организационными мерами и приемами антивирусной защиты.

ОР-6
- навыками работы с программными средствами общего и профессионального назначения;

-навыками ограничения использование ресурсов компьютера на основе раздельного доступа пользователей.</td></tr>
</table>

информационными ресурсами в области обеспечения персоналом ПК-11.6 Организует документооборот по представлению документов по персоналу в государственные органы ПК-11.7 Организует хранение документов в соответствии с требованиями трудового, архивного законодательства Российской Федерации и локальными документами организации			

3. Место дисциплины (модуля) в структуре образовательной программы -

Дисциплина «Информационная безопасность или защита информации» включена в часть формируемую участниками образовательных отношений дисциплины по выбору Б1.В.ДВ.2 учебного плана основной профессиональной образовательной программы высшего образования – программы по направлению подготовки 38.03.03 Управление персоналом, очно-заочной формы обучения.

Дисциплина опирается на результаты обучения, сформированной в рамках школьного курса «Информатика» или соответствующих дисциплин среднего профессионального образования, а также части дисциплины учебного плана изученной обучающимися в первом семестре Информационно-коммуникационные технологии и медиаинформационная грамотность.

Результаты изучения дисциплины «Информационная безопасность или защита информации» являются теоретической и методологической основой для изучения дисциплин: Информационные кадровые технологии, Применение интерактивных средств в профессиональной деятельности, Применение виртуальной и дополненной реальности в профессиональной деятельности, Применение виртуальной и дополненной реальности в профессиональной деятельности, Организация дистанционного взаимодействия в профессиональной деятельности.

4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:

Номер семестра	Учебные занятия						Форма промежуточной аттестации
	Всего		Лекции, час	Лабораторные занятия, час	Самостоят. работа, час	Часов в интерактивной форме	
	Трудоемк.						
	Зач. ед.	Часы					
5	3	108	12	18	78	12	зачёт
Итого:	3	108	12	18	78	12	зачёт

ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1. Указание тем (разделов) и отведенного на них количества академических часов и видов учебных занятий, оформленных в виде таблицы:

Наименование раздела и тем	Количество часов по формам организации обучения			
	Лекц. занятия	Лаб. занятия	Практ. занятия	Самост. работа
5 семестр				
Тема 1. Введение в проблему информационной безопасности	2	2		10
Тема 2. Основы организационно-правового обеспечения информационной безопасности	2	2		8
Тема 3. Угрозы информационной безопасности и методы их реализации.	2	2		8
Тема 4. Составляющие информационной безопасности	1	2		8
Тема 5. Информационная безопасность вычислительных сетей	2	2		8
Тема 6. Компьютерные вирусы и защита от них	0,5	2		8
Тема 7. Стандарты информационной безопасности	1	2		10
Тема 8. Механизмы обеспечения информационной безопасности. Идентификация и аутентификация.	1	2		8
Тема 9. Защита программ и данных	0,5	2		10
Всего:	**12**	**18**		**78**

5.2. Краткое описание содержания тем (разделов) дисциплины

Тема 1. Введение в проблему информационной безопасности.

Понятие информационной безопасности и защищенной системы. Основные принципы защиты информации в компьютерных системах. Основные понятия и определения защиты информации. Основные задачи обеспечения защиты информации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности.

Тема 2. Основы организационно-правового обеспечения информационной безопасности

Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Структура, задачи и основные функции органов государственной власти, отвечающих за организацию защиты персональных данных в РФ.Понятие государственная

тайна. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Тема 3. Угрозы информационной безопасности и методы их реализации.

Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей.

Тема 4. Составляющие информационной безопасности

Основы информационной безопасности. Составляющие информационной безопасности. Конфиденциальность информации. Статическая целостность информации. Динамическая целостность информации. Уровни формирования режима информационной безопасности

Тема 5. Информационная безопасность вычислительных сетей

Особенности обеспечения информационной безопасности в компьютерных сетях.

Сетевые модели передачи данных. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем. Использование защищенных компьютерных систем.

Использование межсетевых экранов (Firewall). Защита виртуальных потоков на различных сетевых уровнях. Защита удаленного доступа к локальной сети. Безопасная доставка E-mail сообщений. Использование ключей и цифровых подписей. Безопасность работы в Интернет с использованием браузера.

Тема 6. Компьютерные вирусы и защита от них.

Понятие разрушающего программного воздействия. Вредоносное ПО. Методы перехвата и навязывания информации. Компьютерные вирусы. Признаки появления вируса. Понятия о видах вирусов, классификация вирусов. Алгоритмическая особенность построения вируса. Вирусная сигнатура. Современные антивирусные программы. Программы «сторожа», ревизоры, доктора, детекторы, вакцины

Тема 7. Стандарты информационной безопасности

Стандарты информационной безопасности. Административный уровень обеспечения информационной безопасности. Классификация угроз информационной безопасности. Администрирование средств безопасности. Политика безопасности информации

Тема 8. Механизмы обеспечения информационной безопасности. Идентификация и аутентификация.

Механизм идентификация и аутентификация пользователей. Криптографические преобразования. Примеры криптографических алгоритмов. Особенности применения криптографических методов. Особенности реализации систем с симметричными и несимметричными ключами. Сравнение симметричных и несимметричных алгоритмов шифрования. Контроль целостности данных. Электронно-цифровая подпись. Использование открытых ключей.

Тема 9. Защита программ и данных

Защита офисных документов. Способы распространения программного обеспечения. Техническая защита от несанкционированного копирования. Базовые методы нейтрализации систем защиты от несанкционированного копирования. Идентификация параметров персонального компьютера. Идентификация жестких дисков. Идентификация гибких дисков. Оценка уникальности конфигурации компьютера. Особенности защиты в операционных системах**.** Подходы к построению защищенной операционной системы. Административные меры защиты. Стандарты защищенности операционных систем. Виды уязвимости и атак на ОС. Классификация угроз безопасности операционной системы.

Тематика рефератов

1. Технология защиты информации и программ.
2. Преступления в сфере информационной безопасности.
3. Компьютерные вирусы и современные методы борьбы с ними.
4. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
5. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
6. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
7. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
8. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
9. Понятие политики безопасности информационных систем. Назначение политики безопасности.
10. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
11. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
12. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
13. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
14. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
15. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
16. Административный уровень защиты информации.
17. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
18. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
19. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
20. Биометрические средства идентификации и аутентификации пользователей.
21. Аутентификация субъектов в распределенных системах, проблемы и решения. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
22. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
23. Законодательный уровень применения цифровой подписи.
24. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
25. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
26. Место информационной безопасности экономических систем в национальной безопасности страны.
27. Концепция информационной безопасности.
28. Средства обеспечения информационной безопасности в ОС Windows. Разграничение доступа к данным. Групповая политика.
29. Определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
30. Причины нарушения безопасности информации при ее обработке криптографическими средствами.

31. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
32. Распределенные информационные системы. Удаленные атаки на информационную систему.
33. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
34. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
35. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.

Перечень учебно-методических изданий кафедры по вопросам организации самостоятельной работы обучающихся

1. Гладких А.А., Сайфутдинов Р.А., Лукьянов В.А. Базовые принципы информационной безопасности. Электронное учебное пособие. УлГПУ 2022 г.
2. Сайфутдинов Р.А., Краснов С.В., Назаров А.Г. и др. Информационные технологии в экономике и управлении. Ульяновск: УлГТУ, 2016.
3. Сайфутдинов Р.А. Неижмак В.В. Информационные технологии в образовании: Учебное пособие – Ульяновск: ФГБОУ ВО «УлГПУ им. И. Н. Ульянова», 2017.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Организация и проведение аттестации бакалавра

ФГОС ВО в соответствии с принципами Болонского процесса ориентированы преимущественно не на сообщение обучающемуся комплекса теоретических знаний, но на выработку у бакалавра компетенций – динамического набора знаний, умений, навыков и личностных качеств, которые позволят выпускнику стать конкурентоспособным на рынке труда и успешно профессионально реализовываться.

В процессе оценки бакалавров необходимо используются как традиционные, так и инновационные типы, виды и формы контроля. При этом постепенно традиционные средства совершенствуются в русле компетентностного подхода, а инновационные средства адаптированы для повсеместного применения в российской вузовской практике.

Цель проведения аттестации – проверка освоения образовательной программы дисциплины-практикума через сформированность образовательных результатов.

Промежуточная аттестация осуществляется в конце семестра и завершает изучение дисциплины; помогает оценить крупные совокупности знаний и умений, формирование определенных компетенций.

7.1. Перечень компетенций, с указанием этапов их формирования в процессе освоения образовательной программы:

Компетенции	**Этапы формирования компетенций**	**Показатели формирования компетенции - образовательные результаты (ОР)**		
		Знать	**Уметь**	**Владеть**
ПК-11 Способен вести кадровое делопроизводство и организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами, владеет навыками составления кадровой отчетности, умеет	**Теоретический (знать)** возможности различных способов сбора, обработки и представления информации, а также их преимущества с учетом современных требований к уровню защиты	ОР-1 - основные понятия информатизации образования; - основы современных технологий сбора, обработки и представления информации;		

обеспечить защиту персональных данных сотрудников ПК-11.1 Знает основы архивного законодательства и нормативные правовые акты Российской Федерации, в части ведения документации по персоналу ПК-11.2 Способен организовывать архивное хранение кадровых документов в соответствии с действующими нормативно-правовыми актами ПК-11.3 Знает технологии, методы и методики проведения анализа и систематизации документов и информации	информации			
	Модельный (уметь) Уметь применять информационные и коммуникационные технологии для сбора, обработки и представления информации в различных форматах, для обработки профессиональных информационных продуктов		ОР-2 - логично выстраивать гуманитарные аспекты информатизации образования	
	Практический (владеть) Владеть навыками использования ИКТ для создания и обработки информации, стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке.			ОР-3 - оценивания влияния информатизации на сферу образования
ПК-11.4 Умеет разрабатывать проекты кадровых документов ПК-11.5 Умеет пользоваться поисковыми системами и информационными ресурсами в области обеспечения персоналом ПК-11.6 Организует документооборот по представлению документов по персоналу в государственные органы ПК-11.7 Организует хранение документов в соответствии с требованиями трудового, архивного законодательства Российской Федерации и локальными документами организации	**Теоретический (знать)** компьютерные технологии, реализующие способы доступа, поиска, отбора информации из электронных баз данных информационно-справочного значения	ОР-4 - основные понятия и составляющие информатизация; образования - основы современных технологий сбора, обработки и представления информации;		
	Модельный (уметь) Уметь использовать современные информационные технологи, осуществлять поиск информации в печатных и электронных источниках, применять средства антивирусной защиты		ОР-5 - логично выстраивать гуманитарные и технологические аспекты информатизации образования	
	Практический (владеть) Владеть навыками			ОР-6 - оценивания влияния

	поиска информации в глобальной информационной сети Интернет и работы с электронными базами данных на русском и иностранном языке			информатизации на сферу образования и изменения механизмов функционирования и реализации системы общего среднего образования в условиях информатизации

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания:

№ п/п	РАЗДЕЛЫ (ТЕМЫ) ДИСЦИПЛИНЫ	Наименование средства, используемого для текущего оценивания образовательного результата	КОД диагностируемого образовательного результата дисциплины					
			ОР- 1	ОР- 2	ОР- 3	ОР- 4	ОР-5	ОР- 6
1.	Тема 1. Введение в проблему информационной безопасности	ОС-1 Доклад выступление	+			+		
2.	Тема 2. Основы организационно-правового обеспечения информационной безопасности	ОС-1 Мини выступление	+	+				
3.	Тема 3. Угрозы информационной безопасности и методы их реализации.	ОС-1 Мини выступление	+		+		+	
4.	Тема 4. Составляющие информационной безопасности	ОС-2		+	+		+	+
5.	Тема 5. Информационная безопасность вычислительных сетей			+	+		+	+
6.	Тема 6. Компьютерные вирусы и защита от них		+	+	+			
7.	Тема 7. Стандарты информационной безопасности			+	+			+
8.	Тема 8. Механизмы обеспечения информационной безопасности. Идентификация и		+	+	+			

	аутентификация.							
9.	Тема 9. Защита программ и данных		+	+	+			+
10.	Контрольная работа, презентация выбранной по теме	ОС-3	+	+	+	+	+	+
11.	Промежуточная аттестация	ОС-4 зачет в форме устного собеседования по вопросам						

Оценочными средствами текущего оценивания являются: устные доклады, защита реферата, итоговой и текущих лабораторных работ, тест по теоретическим вопросам дисциплины. Контроль усвоения материала ведется регулярно в течение всего семестра на лабораторных занятиях.

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

Примерный перечень тем презентаций

1. Технология защиты информации и программ.
2. Преступления в сфере информационной безопасности.
3. Компьютерные вирусы и современные методы борьбы с ними.
4. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
5. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
6. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
7. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
8. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
9. Понятие политики безопасности информационных систем. Назначение политики безопасности.
10. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
11. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
12. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
13. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
14. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
15. Единые критерии безопасности информационных технологий.
16. Административный и процедурный уровень защиты информации.
17. Авторизация пользователей в информационной системе.
18. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
19. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
20. Биометрические средства идентификации и аутентификации пользователей.
21. Аутентификация субъектов в распределенных системах, проблемы и решения.

22. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
23. Электронная цифровая подпись.
24. Место информационной безопасности экономических систем в национальной безопасности страны.
25. Концепция информационной безопасности.
26. Средства обеспечения информационной безопасности в ОС Windows. Разграничение доступа к данным. Групповая политика.
27. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
28. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
29. Распределенные информационные системы. Удаленные атаки на информационную систему.
30. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
31. Вирусы и методы борьбы с ними.
32. Современные антивирусные программы и пакеты.
33. Программно-аппаратные защиты информационных ресурсов в Интернет.
34. Межсетевые экраны, их функции и назначения

Примерный перечень индивидуальных заданий

1. Самостоятельное изучение теоретического материала, не рассматриваемого на лекциях и не представляющего особых сложностей для понимания.
2. Подготовка к семинарским занятиям с конспектированием тематических материалов.
3. Выполнение практических заданий при подготовке к семинарам.
4. Подготовка сообщений и докладов по предложенным темам.
5. Подготовка мультимедийных презентаций.

Примерный перечень вопросов к зачету

1. Основные понятия информационной безопасности. Защита информации. Управление информационной безопасностью. Модель безопасности. Прямое воздействие.
2. Понятие защищенной системы.
3. Как изменялся подход к задаче защите информации? Три этапа развития защиты информации.
4. Теория защиты информации. Основные составные части теории защиты информации.
5. Современная постановка задачи защиты информации.
6. Угроза, атака, источники угроз. Что такое окно опасности. Критерии классификации угроз.
7. Наиболее распространенные угрозы доступности.
8. Программные угрозы доступности.
9. Основные угрозы целостности. Статическая и динамическая целостность.
10. Основные угрозы конфиденциальности.
11. Таксономия угроз безопасности. Что такое уязвимость защиты?. Таксономия угроз безопасности. Ошибки в системах защиты.
12. Что такое компьютерный вирус? Признаки проявления вируса.
13. Классификация компьютерных вирусов – по среде обитания, по степени воздействия, по способам заражения среды обитания, по алгоритмической особенности построения.
14. Что такое антивирусная программа? Вирусная сигнатура. Виды антивирусных программ.
15. Основополагающие принципы решения задачи закрытия каналов несанкционированного доступа.

16. Понятие политики и модели безопасности. Структура монитора обращений.
17. Методы идентификации и аутентификации.
18. Основные функции организационно-правовой базы защиты информации. Виды информационных ресурсов. Какую информацию относят к защищаемой?
19. Признаки защищаемой информации. Владельцы защищаемой информации. Понятие «государственная тайна».
20. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенции.

Краткая характеристика процедуры реализации текущего и промежуточного контроля для оценки компетенций обучающихся представлена в таблице.

№ п/п	Наименование оценочного средства	Краткая характеристика процедуры оценивания компетенций	Представление оценочного средства в фонде
1.	Контрольная работа	Контрольная работа выполняется в форме письменного теста по теоретическим вопросам курса. Регламент – 1- 2 минуты на одно задание.	Тесты по вариантам
2.	Доклад, устное сообщение (мини-выступление)	Доклад - продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-исследовательской или научной темы. Тематика докладов выдается на первых семинарских занятиях, выбор темы осуществляется студентом самостоятельно. Подготовка осуществляется во внеаудиторное время. На подготовку дается одна-две недели. За неделю до выступления студент должен согласовать с преподавателем план выступления. Регламент – 3-5 мин. на выступление. В оценивании результатов наравне с преподавателем принимают участие студенты группы.	Темы докладов
3.	Отчет по итоговой лабораторной работе	Может выполняться индивидуально либо в малых группах (по 2 человека) в аудиторное и во внеаудиторное время (сбор материала по теме работы). Текущий контроль проводится в течение выполнения лабораторной работы. Прием и защита работы осуществляется на последнем занятии или на консультации преподавателя.	Задания для выполнения итоговой лабораторной работы
4.	Защита реферата	Реферат соответствует теме, выдержана структура реферата, изучено 85-100 % источников, выводы четко сформулированы	Темы рефератов
5.	Зачет в форме устного собеседования по вопросам	Проводится в заданный срок, согласно графику учебного процесса. При выставлении оценки учитывается уровень приобретенных компетенций студента. Компонент «знать» оценивается теоретическими вопросами по	Комплект примерных вопросов к экзамену.

		содержанию дисциплины, компоненты «уметь» и «владеть» - практикоориентированными заданиями.	

В конце изучения дисциплины подводятся итоги работы студентов на лекционных и лабораторных занятиях путем суммирования заработанных баллов в течение семестра.

Критерии оценивания знаний обучающихся по дисциплине

Критерии оценивания работы обучающегося по итогам семестра

	Баллы (3 ЗЕ)
«зачтено»	более 150
«не зачтено»	150 и менее

8. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики

Рекомендуемая литература

Основная:

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657 (дата обращения: 19.04.2023). – Режим доступа: по подписке.

2. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2021. — 118 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). — DOI 10.12737/13571. - ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178152 (дата обращения: 19.04.2023). – Режим доступа: по подписке.

3. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 19.04.2023). – Режим доступа: по подписке.

Дополнительная:

1. Гришина, Н. В. Основы информационной безопасности предприятия : учебное пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2021. — 216 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820. - ISBN 978-5-16-015105-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1784437 (дата обращения: 19.04.2023). – Режим доступа: по подписке.

2. Ларин, Д. А. Криптографическая деятельность в России от Полтавы до Бородина : монография / Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2022. — 282 с. — (Научная мысль). — https://doi.org/10.12737/5285. - ISBN 978-5-369-01384-7. - Текст : электронный. -

URL: https://znanium.com/catalog/product/1839706 (дата обращения: 19.04.2023). – Режим доступа: по подписке

3. Бабаш, А. В. История защиты информации в зарубежных странах : учебное пособие / А.В. Бабаш, Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2021. — 284 с. — (Высшее образование). — DOI: https://doi.org/10.12737/15090. - ISBN 978-5-369-01844-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1215133 (дата обращения: 19.04.2023). – Режим доступа: по подписке.

Интернет-ресурсы

- «Информационные технологии для новой школы»: Материалы международной конференции) / [Электронный ресурс]. Режим доступа: http://conf.rcokoit.ru/.
- «Информационные технологии». Ежемесячный теоретический и прикладной научно-технический журнал (с приложением) / [Электронный ресурс]. Режим доступа: http://novtex.ru/IT/index.htm.
- Информационные технологии в образовании. / [Электронный ресурс]. Режим доступа http://physics.herzen.spb.ru/teaching/materials/gosexam/b25.htm.
- Цифровая грамотность для гуманитарных направлений / [Электронный ресурс]. Режим доступа: https://openedu.ru/course/hse/DIGLIT_2/
- «ENGLISH VOYAGE». Сервис для изучения английского языка / [Электронный ресурс]. Режим доступа: http://englishvoyage.com/
- «LEOnetwork» Материалы для изучения английского в разных форматах: уроках, играх, общении в чатах и т. п. / [Электронный ресурс]. Режим доступа: https://www.learnenglish.de/
- Die Seite für den Deutschunterricht / [Электронный ресурс]. Режим доступа: https://www.grammatikdeutsch.de/

10. Методические указания для обучающихся по освоению дисциплины (модуля)

Успешное изучение курса требует от обучающихся посещения лекций, активной работы на лабораторных занятиях, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой.

Запись **лекции** – одна из форм активной самостоятельной работы обучающихся, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. В конце лекции преподаватель оставляет время (5 минут) для того, чтобы обучающиеся имели возможность задать уточняющие вопросы по изучаемому материалу. Из-за недостаточного количества аудиторных часов некоторые темы не удается осветить в полном объеме, поэтому преподаватель, по своему усмотрению, некоторые вопросы выносит на самостоятельную работу студентов, рекомендуя ту или иную литературу. Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям. В случае необходимости обращаться к преподавателю за консультацией.

Подготовка к **лабораторным занятиям**.

При подготовке к лабораторным занятиям студент должен изучить теоретический материал по теме занятия (использовать конспект лекций, изучить основную литературу, ознакомиться с дополнительной литературой, при необходимости дополнить конспект, делая в нем соответствующие записи из литературных источников). В случае затруднений, возникающих при освоении теоретического материала, студенту следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В начале лабораторного занятия преподаватель знакомит студентов с темой, оглашает

план проведения занятия, выдает задание. В течение отведенного времени на выполнение работы студент может обратиться к преподавателю за консультацией или разъяснениями. В конце занятия проводится прием выполненных работ, собеседование со студентом.

Результаты выполнения лабораторных работ оцениваются в баллах, в соответствии с балльно-рейтинговой системой университета.

Подготовка к **устному докладу**.

Доклады делаются по теме №1 с целью проверки теоретических знаний обучающегося, его способности самостоятельно приобретать новые знания, работать с информационными ресурсами и извлекать нужную информацию.

Доклады заслушиваются в начале лабораторного занятия после изучения темы. Продолжительность доклада не должна превышать 5 минут. Тему доклада студент выбирает по желанию из предложенного списка.

При подготовке доклада студент должен изучить теоретический материал, используя основную и дополнительную литературу, обязательно составить план доклада (перечень рассматриваемых им вопросов, отражающих структуру и последовательность материала), подготовить раздаточный материал или презентацию. План доклада необходимо предварительно согласовать с преподавателем.

Выступление должно строиться свободно, убедительно и аргументировано. Преподаватель следит, чтобы выступление не сводилось к простому воспроизведению текста, не допускается простое чтение составленного конспекта доклада. Выступающий также должен быть готовым к вопросам аудитории и дискуссии.

Выполнение **лабораторной работы**.

Для закрепления практических навыков по использованию информационных технологий в образовании студенты выполняют практические задания под руководством преподавателя.

Текущая проверка разделов работы осуществляется в ходе выполнения работы на занятиях и на консультациях. Выполнение практической контрольной работы проводится на последнем занятии. Для оказания помощи в самостоятельной работе проводятся индивидуальные консультации.

Подготовка к тесту.

При подготовке к тесту необходимо изучить теоретический материал по дисциплине. С целью оказания помощи студентам при подготовке к тесту преподавателем проводится групповая консультация с целью разъяснения наиболее сложных вопросов теоретического материала.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

* Архиватор 7-Zip,
* Антивирус ESET NOD32 Business Edition renewal,
* Операционная система Windows 7 Pro,
* Офисный пакет программ Microsoft Office 2010- Professional ,
* Программа Pascal ABC
* Программа для просмотра файлов формата DjVuWinDjView,
* Браузер GoogleChrome.

12.Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего**

		документа
По. 100-летия со дня рождения Ленина, дом . Аудитория № 419 Компьютерный класс. Аудитория для практических занятий.	Стулья – 20 шт., парты – 10 шт., меловая доска – 1 шт., доска белая магнитная WBASO912 – 1 шт., компьютер в сборе Intel– 8 шт., проектор NEC M361X – 1 шт.	* Архиватор 7-Zip, открытое программное обеспечение, бесплатная лицензия, пролонгировано. * Антивирус ESET Endpoint Antivirus for Windows, лицензия EAV-0120085134, контракт №1110 от 15.12.2014 г., действующая лицензия. * Операционная система Windows Pro 7 RUS Upgrd OLP NL Acdmc, Open License: 47357816, Гражданско-правовой договор № 0368100013813000050-0003977-01 от 02.10.2013 г., действующая лицензия. * Офисный пакет программ Microsoft Office Professional 2013 OLP NL Academic, Open License: 62135981, договор № 799 от 25.09.2013 г., действующая лицензия. * Программа для просмотра файлов формата DjVu WinDjView, открытое программное обеспечение, бесплатная лицензия, пролонгировано. * Программа для просмотра файлов формата PDF Adobe Reader XI, открытое программное обеспечение, бесплатная лицензия, пролонгировано. * Браузер Google Chrome, открытое программное обеспечение, бесплатная лицензия, пролонгировано.

Лист согласования рабочей программы
учебной дисциплины (практики)

Направление подготовки: 38.03.03 Управление персоналом
Профиль:
Рабочая программа Информационная безопасность или защита информации
Составитель: Сайфутдинов Р.А. – Ульяновск: УлГПУ, 2023.

Программа составлена с учетом федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.03.03 Управление персоналом, утверждённого Министерством образования и науки Российской Федерации, и в соответствии с учебным планом.

Составитель _____ Сайфутдинов Р.А.
(подпись)

Рабочая программа учебной дисциплины (практики) одобрена на заседании кафедры информатики «23» мая 2023 г., протокол № 9

Заведующий кафедрой _____ Шубович В.Г. 23.05.23
личная подпись *расшифровка подписи* *дата*

Рабочая программа учебной дисциплины (практики) согласована с библиотекой

Сотрудник библиотеки
_____ Маркова Ю.Б. 23.05.23
личная подпись *расшифровка подписи* *дата*

Программа рассмотрена и одобрена на заседании ученого совета факультета права, экономики и управления
"30" 05 2023 г., протокол № 9

Председатель ученого совета факультета права, экономики и управления
_____ Макарова 30.05.23
личная подпись *расшифровка подписи* *дата*