Министерство образования и науки 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

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ И.О. Петрищев
«_30_» _августа_____ 2017 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Программа учебной дисциплины вариативной части

для направления подготовки
44.04.01 Педагогическое образование
(шифр и наименование)
направленность (профиль) образовательной программы
Информационные технологии в образовании
(заочная форма обучения)

Составитель: Шубович В.Г.,
доктор педагогических наук,
кандидат технических наук,
профессор кафедры информатики

Рассмотрено и утверждено на заседании ученого совета факультета физико-математического и технологического образования, протокол от «_04_» _июля_2017 г. № 11

Ульяновск, 2017

1. Наименование дисциплины

Дисциплина «Информационная безопасность» дисциплиной по выбору основной профессиональной образовательной программы высшего образования.

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

Целью освоения дисциплины «Информационная безопасность» является прочное и сознательное овладение студентами знаниями и умениями работы с прикладными программами, применением информационных технологий, которые необходимы современному специалисту для осуществления профессиональной деятельности

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

Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Компетенции	знает	умеет	владеет навыками
Готовностью использовать знание современных проблем науки и образования при решении профессиональных задач **(ОПК -2)**	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-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-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.

Способностью формировать образовательную среду и использовать профессиональные знания и умения в реализации задач инновационной образовательной политики **(ПК -2)**	ОР-4 - основы современных технологий сбора, обработки и представления информации;	ОР-5 - использовать современные информационно-коммуникационные технологии (включая пакеты прикладных программ, локальные и глобальные компьютерные сети) для сбора, обработки и анализа информации.	ОР-6 - навыками работы с программными средствами общего и профессионального назначения; -навыками ограничения использование ресурсов компьютера на основе раздельного доступа пользователей.

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

Дисциплина «Информационная безопасность» является дисциплиной по выбору основной профессиональной образовательной программы высшего образования 44.04.01 Педагогическое образование, заочной формы обучения

Дисциплина опирается на результаты обучения, сформированные в рамках школьного курса «Информатика и ИКТ» или соответствующих дисциплин среднего профессионального образования, а также части дисциплины учебного плана изученной обучающимися во втором семестре.

Результаты изучения дисциплины «Информационная безопасность» являются теоретической и методологической основой для изучения дисциплин: Информационная безопасность, письменный перевод информационных текстов, устный последовательный перевод информационных текстов, практика по получению профессиональных умений и опыта 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:

5.

Номер семестра	Учебные занятия						Форма промежуточной аттестации
	Всего Трудоемк.		Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	
	Зач. ед.	Часы					
4	2	72	2	-	6	58	зачет
Итого:	2	72	2	-	6	58	зачет

ПРИМЕРНЫЙ ТЕМАТИЧЕСКИЙ ПЛАН

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

6.1. 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	Объем уч. раб. с прим. интеракт. форм
4 семестр					
Тема 1. Введение в проблему информационной безопасности	1			8	1
Тема 2. Основы организационно-правового обеспечения информационной безопасности	1			10	2
Тема 3. Угрозы информационной безопасности и методы их реализации**.**		2		10	1
Тема 4. Методы и средства обеспечения информационной безопасности информационных систем		2		10	1
Тема 5. Использование защищенных компьютерных систем.		1		10	1
Тема 6. Компьютерные вирусы и защита от них. Защита от разрушающих программных воздействий.		1		10	1
Всего:	2	6		58	12 (20,5%)

6.2. 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.

Необходимость защиты информационных систем. Технические предпосылки кризиса информационной безопасности. Этапы развития защиты информации. Современная постановка задачи защиты информации. Основные задачи обеспечения защиты информации.

Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности.

Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена.

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.

Виды информационных ресурсов. Открытая, запатентованная и защищаемая информация. Владельцы защищаемой информации. Понятие государственная тайна. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг.

Компьютерные преступления. Организационное обеспечение информационной безопасности.

Тема 3. Угрозы информационной безопасности и методы их реализации.

Три вида возможных нарушений информационной системы. Понятие угрозы Виды противников или "нарушителей". Окно опасности. Классификация видов угроз информационной безопасности по различным признакам. Угрозы доступности, целостности и конфиденциальности.

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.

Причины нарушения безопасности вычислительных систем. Таксономия угроз безопасности. Уязвимость защиты. Ошибки в системах защиты. Этапы появления ошибок защиты. Компоненты систем, где чаще всего проявляются ошибки защиты.

Тема 4. Методы и средства обеспечения информационной безопасности информационных систем

Общая проблема информационной безопасности информационных систем. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение). Основные технологии построения защищенных экономических информационных систем (ЭИС).

Защита информации от несанкционированного доступа. Контроль доступа пользователей к ресурсам ИС. Монитор обращений. Структура монитора обращений. Идентификация и аутентификация пользователей ИС. Способы аутентификации.

Математические и методические средства защиты. Компьютерные средства реализации защиты в информационных системах.

Тема 5. Использование защищенных компьютерных систем.

Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем. Использование защищенных компьютерных систем. Стандарты по оценке защищенных систем. Примеры практической реализации.

Тема 6. Компьютерные вирусы и защита от них. Защита от разрушающих программных воздействий.

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.

Материалы, используемые для текущего контроля успеваемости обучающихся по дисциплине

Контрольные вопросы

1. Что можно сделать для предотвращения несанкционированного просмотра документа Microsoft Excel?
2. Что можно сделать для предотвращения несанкционированного изменения документа Microsoft Excel?
3. Чем отличается защиты файла от изменений и защита книги от изменений?
4. В каких ситуациях целесообразно защищать от изменений только часть ячеек листа?
5. Что дает добавление цифровой подписи к файлу?
6. Что можно сделать для предотвращения утраты данных в результате случайного повреждения пользователем?
7. В каких ситуациях следует рекомендовать открытие файла в режиме «только чтение»?
8. Какие действия можно выполнять в книге, открытой только для чтения?
9. Что такое «резервная копия файла» и как она образуется?
10. Что необходимо делать для обеспечения защиты компьютера от компьютерных вирусов?
11. Чем отличаются уровни безопасности, устанавливаемые при работе с файлами в Microsoft Excel?
12. Что такое «список надежных источников», и для каких целей можно его использовать?
13. Что можно сделать для предотвращения утраты данных при зависании компьютера или внезапном отключении питания?
14. Можно ли пользоваться автосохранением вместо обычного сохранения файлов?

Практическое задание.

В среде электронной таблицы Microsoft Excel создать таблицу и выполнить необходимые расчеты. Графически представить указанные данные. Защитить представленную информацию.

Ведомость учета сроков и сумм кредитов по предприятиям в 2017 году

Определить:

1. Возвращенную сумму $S = P*(1+\frac{d2-d1}{\hat{E}}*i)$, $,

где K – продолжительность года в днях (принять K = 365).

2. Продолжительность периода начисления в годах $n = \frac{S-P}{P*i\%}$ и общую сумму процентных денег за весь период начисления $I = S - P$.
3. Представить в виде объемной диаграммы (гистограммы) зависимость продолжительности периода начисления по фирмам и в виде объемной круговой разрезанной диаграммы – зависимость общей суммы процентных денег по фирмам.

Название предприятия	Размер ссуды, $ (P)	Дата		Относительная величина ставки процентов, % (i)	Возвращенная сумма, $ (S)	Продолжительность периода начисления в годах (n)	Общая сумма процентных денег за весь период начисления, $ (I)
		выдачи кредита ($d1$)	погашения кредита ($d2$)				
	100 000	01.фев	03.дек	18			
	5 000 000	15.фев	21.ноя	20			
	350 000	03.мар	30.дек	15			
	7 000 000	12.янв	06.окт	11			
	10 000 00	07.апр	14.сен	17			
Итого					xxx	xxx	xxx

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.

Примерный перечень тем индивидуальных лабораторных работ:

1. Защита информации от несанкционированного просмотра и изменения:

- уровни защиты информации от просмотра и изменения.
- защита доступа с использованием паролей.
- процедуры защиты файлов, отдельных листов, строк и столбцов листов от несанкционированного просмотра.

2. Защита информации от случайного повреждения и макровирусов.

- способы предотвращения случайного повреждения и утраты данных пользователем.
- возможности защиты файлов, в том числе, путем создания резервной копии.
- возможность защиты книг, листов и элементов листов.
- особенности макровирусов.
- уровни защиты от макровирусов.
- формирование надежных источников файлов.
- ситуации работы с файлами, содержащими макросы, при различных уровнях защиты.
- возможность защиты информации от утраты при зависании компьютера или внезапном отключении питания.

3. Средства защиты файлов в MS Office, методы защиты документов Microsoft Office.
   - защита от изменений документа.
   - защита от записи документа.
   - защита на открытие документа.

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

1. Сайфутдинов Р.А., Краснов С.В., Назаров А.Г. и др. Информационные технологии в экономике и управлении. Ульяновск: УлГТУ, 2016. .
2. Сайфутдинов Р.А. Неижмак В.В. Информационные технологии в образовании: Учебное пособие – Ульяновск: ФГБОУ ВО «УлГПУ им. И. Н. Ульянова», 2017.

7. 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**
ОПК-2 Готовностью использовать знание современных проблем науки и образования при решении профессиональных задач	**Теоретический (знать)** возможности различных способов сбора, обработки и представления информации, а также их преимущества с учетом современных требований к уровню защиты информации	ОР-1 - основные понятия информатизации образования; - основы современных технологий сбора, обработки и представления 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			ОР-3 - оценивания влияния информатизации на сферу

	информации, стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке.			образования
ПК-2 Способностью формировать образовательную среду и использовать профессиональные знания и умения в реализации задач инновационной образовательной политики	**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 поиска информации в глобальной информационной сети Интернет и работы с электронными базами данных на русском и иностранном языке			ОР-6 - оценивания влияния 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.	Введение в проблему информационной безопасности	ОС-1 Доклад выступление	+			+		
2.	Основы организационно-правового обеспечения информационной безопасности	ОС-1 Мини выступление	+	+				
3.	Угрозы информационной безопасности и методы их реализации**.**	ОС-1 Мини выступление	+		+		+	
4.	Методы и средства обеспечения информационной безопасности информационных систем	ОС-2		+	+		+	+
5.	Использование защищенных компьютерных систем.			+	+		+	+
6.	Компьютерные вирусы и защита от них. Защита от разрушающих программных воздействий.		+	+	+			
7.	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.

Критерии и шкалы оценивания

ОС-1 Доклад-выступление

Критерии и шкала оценивания

Критерий	Этапы формирования компетенций	Максимальное количество баллов
Знает источники и классификацию угроз информационной безопасности;	Модельный (уметь)	6
Знает основные средства и способы защиты	Модельный (уметь)	6

информации при работе на компьютере.		
Всего		12

ОС-2 Защита итоговой лабораторной работы

Критерий	Этапы формирования компетенций	Максимальное количество баллов
Умеет применять правовые, организационные, технические и программные средства защиты информации	Модельный (уметь)	4
Умеет создавать программные средства защиты информации.	Модельный (уметь)	4
Умеет использовать современные информационно-коммуникационные технологии для сбора, обработки и анализа информации.	Практический (владеть)	4
Всего:		**12**

ОС-3 Контрольная работа

Критерии и шкала оценивания

Критерий	тапы формирования компетен	Шкала оценивания (максимальное количество баллов)
Знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, источники и классификацию угроз информационной безопасности	Модельный (уметь)	7
Умеет применять правовые, организационные, технические и программные средства защиты информации;	Модельный (уметь)	8
Умеет использовать современные информационно-коммуникационные технологии (включая пакеты прикладных программ, локальные и глобальные компьютерные сети) для сбора, обработки и анализа информации.	Модельный (уметь)	8
Владеет методами защиты информации при работе с компьютерными системами и организационными мерами и приемами антивирусной защиты.	Практический (владеть	10
Всего		32

ОС-4 Зачет в форме устного собеседования по вопросам

При проведении зачета учитывается уровень знаний обучающегося при ответах на вопросы (теоретический этап формирования компетенций), умение обучающегося отвечать на дополнительные вопросы по применению теоретических знаний на практике и по выполнению обучающемся заданий текущего контроля (модельный этап формирования компетенций).

Критерии и шкала оценивания зачета:

Критерий	Этапы формирования компетенций	Количество баллов
Обучающийся знает источники и классификацию угроз информационной безопасности; - основные средства и способы защиты информации при работе на компьютере;	Теоретический (знать)	0-10

- правовые основы организации защиты государственной тайны и конфиденциальной информации		
Обучающийся умеет - применять правовые, организационные, технические и программные средства защиты информации; - применять правовые, организационные, технические и программные средства защиты информации.	Модельный (уметь)	11-21
Обучающийся владеет - программными методами защиты информации при работе с компьютерными системами и организационными мерами и приемами антивирусной защиты; -	Практический (владеть)	22-32

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 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.
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.
6. Выполнение самостоятельных работ.
7. Написание рефератов.

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, 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	Проводится в заданный срок, согласно графику	Комплект примерных

	устного собеседования по вопросам	учебного процесса. При выставлении оценки учитывается уровень приобретенных компетенций студента. Компонент «знать» оценивается теоретическими вопросами по содержанию дисциплины, компоненты «уметь» и «владеть» - практикоориентированными заданиями.	вопросов к экзамену.

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

№ п/п	Вид деятельности	Максимальное количество баллов за одно занятие	Максимальное количество баллов по дисциплине
1.	Посещение лекций	1	6
2.	Посещение занятий	1	10
3.	Работа на занятии: - выполнение лабораторной работы; - работа у доски; - результат выполнения домашней работы	12 7 3 2	120
4.	Контрольное мероприятие		32
5.	Зачёт		32
ИТОГО:	2 зачетных единицы		200 баллов

Формирование балльно-рейтинговой оценки работы обучающихся

		Посещение лекций	Посещение лабораторных занятий	Работа на лабораторных занятиях	Контроль-ная работа	Зачет
8 семестр	Разбалловка по видам работ	6 х 1=6 баллов	10 х 1=10 баллов	12 х 10=120 баллов	32 балла	32 балла
	Суммарный макс. балл	6 балла max	16 баллов max	136 баллов max	168 баллов max	200 баллов max

Критерии оценивания работы обучающегося по итогам семестра

По итогам изучения, трудоёмкость которой составляет 2 ЗЕ и изучается в 8 семестре, обучающийся набирает определённое количество баллов, которое соответствует «зачтено» или «незачтено» согласно следующей таблице:

Отметка	**Баллы (2 ЗЕ)**
«зачтено»	Более 60
«незачтено»	Менее 60

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Баранова Е. К.Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.: 60х90 1/16. - (Высшее образование) (Переплёт) ISBN 978-5-369-01450-9 (Электронный ресурс. – Режим доступа http://znanium.com/bookread2.php?book=495249)
2. Глинская Е. В.Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/ГлинскаяЕ.В., ЧичваринН.В. - М.: НИЦ ИНФРА-М, 2016. - 118 с.: 60х90 1/16. - (Высшее образование:Бакалавриат) (Обложка) ISBN 978-5-16-010961-9, 300 экз. (Электронный ресурс. – Режим доступа http://znanium.com/bookread2.php?book=507334)
3. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. (Электронный ресурс. – Режим доступа http://znanium.com/catalog.php?bookinfo=420047)

Дополнительная литература

1. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. (Электронный ресурс. – Режим доступа http://znanium.com/catalog.php?bookinfo=335362)
2. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. (Электронный ресурс. – Режим доступа http://znanium.com/catalog.php?bookinfo=491597)
3. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. (Электронный ресурс. – Режим доступа http://znanium.com/catalog.php?bookinfo=463061)

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы

1. Компьютерные технологии в науке и образовании: Учебное пособие / Л.С. Онокой, В.М. Титов. - М.: ИД ФОРУМ: ИНФРА-М, 2011. - 224 с. (Электронный ресурс. – Режим доступа: http://znanium.com/catalog.php?bookinfo=241862).
2. Максимов Н. В. Информационные технологии в профессиональной деятельности: учебное пособие / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2010. - 496 с. [Электронный ресурс]- Режим доступа http://znanium.com/catalog.php?bookinfo=180612
3. Информационные технологии в науке и образовании: Учебное пособие / Е.Л. Федотова, А.А. Федотов. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2015. - 336 с. (Электронный ресурс. – Режим доступа http://znanium.com/bookread2.php?book=487293. (Электронный ресурс. – Режим доступа http:// biblio-club.ru/index.php?page=book_view_red&book_id=230535).
4. Трайнев, В. А. Новые информационные коммуникационные технологии в образовании [Электроный ресурс] / В.А. Трайнев, В. Ю. Теплышев, И. В. Трайнев. - 2-е изд. - М. : Издательско-торговая корпорация “Дашков и К°”, 2013. - 320 с. (Электронный ресурс. – Режим доступа http://znanium.com/bookread2.php?book=430429)
5. Информационные технологии в науке и образовании: Учебное пособие / Е.Л. Федотова, А.А. Федотов. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 336 с. (Электронный ресурс. – Режим доступа http://znanium.com/bookread2.php?book=411182.

Электронные библиотечные системы (ЭБС), с которыми сотрудничает «УлГПУ им. И.Н. Ульянова»

№	Название ЭБС	№, дата договора	Срок использования	Количество пользователей
1	«ЭБС ZNANIUM.COM»	Договор № 2304 от 19.05.2017	с 31.05.2017 по 31.05.2018	6 000
2	ЭБС «Университетская библиотека онлайн»	Договор № 1010 от 26.07.2016	с 22.08.2016 по 21.11.2017	6 000

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.