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

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ С.Н. Титов
«25» июня 2021 г.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Программа учебной дисциплины модуля
«Информационная безопасность»

основной профессиональной образовательной программы высшего образования – программы магистратуры по направлению подготовки
44.04.01 Педагогическое образование

направленность (профиль) образовательной программы
«Информационные технологии в образовании»

(заочная форма обучения)

Составитель: Сайфутдинов Р.А.
Доцент кафедры Информатики

Рассмотрено и утверждено на заседании ученого совета факультета физико-математического и технологического образования, протокол от «21» июня 2021 г. №7

Ульяновск, 2021

Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к дисциплинам по выбору вариативного модуля учебного плана основной профессиональной образовательной программы высшего образования – программы магистратуры по направлению подготовки 44.04.01 Педагогическое образование, направленность (профиль) образовательной программы: Информационные технологии в образовании, заочной формы обучения.

Дисциплина опирается на результаты обучения, сформированные в рамках изучения дисциплин и прохождения практик: Методология исследования в образовании, Методический модуль, Педагогический модуль, Актуальные вопросы экономических процессов, Учебная практика (научно-исследовательская работа), Учебная практика (практикум по программированию).

Результаты изучения дисциплины являются основой для изучения дисциплин и прохождения практик: Научно-исследовательский модуль, Производственная практика (НИР: Моделирование и прогнозирование процессов в образовании).

1. Перечень планируемых результатов обучения (образовательных результатов) по дисциплине

Целью освоения дисциплины «Информационная безопасность» является формирование знаний связанных с обеспечением информационной безопасности и защиты информации. **Задачей** освоения дисциплины является формирование знаний об угрозах информационной безопасности, умение выявлять угрозы информационной безопасности, использовать нормативно-правовые акты по информационной безопасности, использовать методы и средства обеспечения информационной безопасности.

В результате освоения программы магистратуры обучающийся должен овладеть следующими результатами обучения по дисциплине «Информационная безопасность» (в таблице представлено соотнесение образовательных результатов обучения по дисциплине с индикаторами достижения компетенций):

Компетенция и индикаторы ее достижения в дисциплине	Образовательные результаты дисциплины (этапы формирования дисциплины)		
	знает	умеет	владеет

УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий ИУК 1.1. Выявляет проблемную ситуацию в процессе анализа проблемы, определяет этапы ее разрешения с учетом вариативных контекстов. ИУК 1.2. Находит, критически анализирует и выбирает информацию, необходимую для выработки стратегии действий по разрешению проблемной ситуации. ИУК1.3. Рассматривает	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.
различные варианты решения проблемной ситуации на основе системного подхода, оценивает их преимущества и риски. ИУК 1.4. Грамотно, логично, аргументированно формулирует собственные суждения и оценки. Предлагает стратегию действий. ИУК 1.5. Определяет и оценивает практические последствия реализации действий по разрешению проблемной ситуации			

2. Объем дисциплины 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	Практические занятия, час	Лабораторные занятия, час	Самостоят. работа, час	
	Трудоемк.						
	Зач. ед.	Часы					

3	3	108	4	20	-	84	зачёт
Итого:	3	108	4	20	-	84	зачёт

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

3. 1.Указание тем (разделов) и отведенного на них количества академических часов и видов учебных занятий

Наименование раздела и тем	Количество часов по формам организации обучения			
	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятель-ная работа
3 семестр				
Тема 1. Введение в проблему информационной безопасности	2	-	-	14
Тема 2. Основы организационно-правового обеспечения информационной безопасности	2	4	-	14
Тема 3. Угрозы информационной безопасности и методы их реализации**.**	-	4	-	14
Тема 4. Методы и средства обеспечения информационной безопасности информационных систем	-	4	-	14
Тема 5. Использование защищенных компьютерных систем.	-	4	-	14
Тема 6. Компьютерные вирусы и защита от них. Защита от разрушающих программных воздействий.	-	4	-	14
Итого по 3 семестру	**4**	**20**	**-**	**84**

3.2. Краткое описание содержания тем (разделов) дисциплины Краткое содержание курса (3 семестр)

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. Задачи в сфере обеспечения информационной безопасности на уровне государства.

Интерактивная форма: «Работа в группе» **Тема 3. Угрозы информационной безопасности и методы их реализации.**

Классификация видов угроз информационной безопасности по различным признакам. Угрозы доступности, целостности и конфиденциальности. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей.

Интерактивная форма: «Работа в группе» **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). Защита информации от несанкционированного доступа. Контроль доступа пользователей к ресурсам ИС. Компьютерные средства реализации защиты в информационных системах.

Интерактивная форма: «Работа в группе»

Тема 5. Использование защищенных компьютерных систем.

Политика безопасности. Критерии и классы защищенности средств вычислительной техники. Стандарты по оценке защищенных систем.

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

Компьютерные вирусы. Понятия о видах вирусов, классификация вирусов. Алгоритмическая особенность построения вируса. Вирусная сигнатура. Современные антивирусные программы. Программы «сторожа», ревизоры, доктора, детекторы, вакцины.

Интерактивная форма: «Работа в группе»

4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Самостоятельная работа студентов является особой формой организации учебного процесса, представляющая собой планируемую, познавательно, организационно и методически направляемую деятельность студентов, ориентированную на достижение конкретного результата, осуществляемую без прямой помощи преподавателя. Самостоятельная работа студентов является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, а также выполнение учебных заданий, подготовку к предстоящим занятиям и зачету. Она предусматривает, как правило, разработку рефератов, написание докладов, выполнение индивидуальных заданий в соответствии с рабочей программой дисциплины. Тема для такого выступления может быть предложена преподавателем или избрана самим студентом, но материал выступления не должен дублировать лекционный материал. Реферативный материал служит дополнительной информацией для работы на практических занятиях. Основная цель данного вида работы состоит в обучении студентов методам самостоятельной работы с учебным материалом. Для полноты усвоения тем, вынесенных в практические занятия, требуется работа с первоисточниками. Курс предусматривает самостоятельную работу студентов со специальной литературой. Следует отметить, что самостоятельная работа

студентов результативна лишь тогда, когда она выполняется систематически, планомерно и целенаправленно.

Задания для самостоятельной работы предусматривают использование необходимых терминов и понятий по проблематике курса. Они нацеливают на практическую работу по применению изучаемого материала, поиск библиографического материала и электронных источников информации, иллюстративных материалов. Задания по самостоятельной работе даются по темам, которые требуют дополнительной проработки.

Самостоятельная работа осуществляется в формах:

- подготовки к устным докладам (мини-выступлениям);
- подготовка к защите рефератов;
- выполнение индивидуальных практических заданий.

Темы рефератов (задания для контрольной работы)

1. Концепция информационной безопасности в РФ.
2. Место информационной безопасности экономических систем в национальной безопасности страны.
3. Федеральный закон "Об информации, информационных технологиях и о защите информации
4. Кибербезопасность на современном этапе.
5. Принципы информационной безопасности вычислительных систем.
6. Зарубежный опыт в области защиты информации.
7. Преступления в сфере информационной безопасности.
8. Компьютерные вирусы и современные методы борьбы с ними.
9. Классификация угроз информационной безопасности.
10. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
11. Понятие политики безопасности информационных систем. Назначение политики безопасности.
12. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
13. Электронная цифровая подпись.
14. Программно-аппаратные защиты информационных ресурсов в Интернет.
15. Физические средства обеспечения информационной безопасности.
16. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
17. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
18. Структура требований безопасности. Классы защищенности.

Для самостоятельной подготовки к занятиям по дисциплине рекомендуется использовать учебно-методические материалы:

1. Гладких А.А., Сайфутдинов Р.А. Базовые принципы информационной безопасности. Электронное учебное пособие. Ульяновск: УлГТУ, 2017.
2. Сайфутдинов Р.А., Краснов С.В., Назаров А.Г. и др. Информационные технологии в экономике и управлении. Учебное пособие. Ульяновск: УлГТУ, 2016. .

5. Примерные оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Организация и проведение аттестации магистранта

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

В процессе оценки обучающихся 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.

Оценочными средствами текущего оценивания являются: доклад, тесты по теоретическим вопросам дисциплины, защита практических работ и т.п. Контроль усвоения материала ведется регулярно в течение всего семестра на практических занятиях.

№ п/п	**СРЕДСТВА ОЦЕНИВАНИЯ,** используемые для текущего оценивания показателя формирования компетенции	Образовательные результаты дисциплины
	Оценочные средства для текущей аттестации ОС-1 Защита реферата ОС-2 Отчет о выполнении индивидуального практического задания и его защита	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
	Оценочные средства для промежуточной аттестации зачет (экзамен) ОС-3 Зачет в форме устного собеседования по вопросам	

		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; Применять средства защиты данных от разрушающих воздействий компьютерных вирусов; Владеть базовыми программными методами защиты информации при работе с компьютерными системами, организационными мерами и приемами антивирусной защиты.

Описание оценочных средств и необходимого оборудования (демонстрационного материала), а также процедуры и критерии оценивания индикаторов достижения компетенций на различных этапах их формирования в процессе освоения образовательной программы представлены в Фонде оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Информационная безопасность».

Материалы, используемые для текущего контроля успеваемости обучающихся по дисциплине

Материалы для организации текущей аттестации представлены в п.5 программы.

Материалы, используемые для промежуточного контроля успеваемости обучающихся по дисциплине

ОС-3 Зачет в форме устного собеседования по вопросам

Перечень вопросов к зачету

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 программноаппаратных 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

Критерии оценивания знаний обучающихся по дисциплине

Формирование балльно-рейтинговой оценки работы обучающихся

		Посещение лекций	Посещение практических занятий	Работа на практических занятиях	зачет
3 семестр	Разбалловка по видам работ	2 х 1=2 баллов	10 х 1=10 баллов	229 баллов	64 балла
	Суммарный макс. балл	2 балла max	12 баллов max	236 баллов max	300 баллов max

Критерии оценивания работы обучающегося по итогам семестра

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

6. Методические указания для обучающихся по освоению дисциплины

Успешное изучение курса требует от обучающихся посещения лекций, активной работы на практических 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 практическим занятиям.**

При подготовке к практическим 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 практического занятия преподаватель знакомит студентов с темой, оглашает план проведения занятия, выдает задания. В течение отведенного времени на выполнение работы студент может обратиться к преподавателю за консультацией или разъяснениями. В конце занятия проводится прием выполненных заданий, собеседование со студентом.

Результаты выполнения практических зданий оцениваются в баллах, в соответствии с балльно-рейтинговой системой университета.

Планы практических занятий (3 семестр)

Практическое задание № 1. Основы организационно-правового обеспечения информационной безопасности План:

1. Открытая, запатентованная и защищаемая информация.
2. Владельцы защищаемой информации.
3. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
4. Особенности сертификации и стандартизации криптографических услуг.
5. Компьютерные преступления. Организационное обеспечение информационной безопасности.

Практическое задание № 2. Угрозы информационной безопасности и методы их реализации**.**

План:

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

Практическое задание № 3. Методы и средства обеспечения информационной безопасности информационных систем План:

1. Защита информации от несанкционированного доступа. Контроль доступа пользователей к ресурсам ИС.
2. Использование ключей и цифровых подписей.
3. Способы противодействия несанкционированному сетевому и межсетевому доступу.
4. Идентификация и аутентификация пользователей ИС.
5. Математические и методические средства защиты.

Практическое задание № 4. Использование защищенных компьютерных систем.

План:

1. Компьютерные средства реализации защиты в информационных системах 2. Противодействие несанкционированному межсетевому доступу.
3. Использование межсетевых экранов (Firewall).
4. Защита информации от несанкционированного просмотра и изменения.
5. Защита доступа с использованием паролей

Практическое задание № 5. Компьютерные вирусы и защита от них.

План

1. Современные антивирусные программы.

2. Защита информации от случайного повреждения и макровирусов 3. Защита от разрушающих программных воздействий
4. Использование межсетевых экранов (Firewall).
5. Безопасная доставка E-mail сообщений.
6. Средства защиты файлов в MSOffice.

7. **Перечень основной и дополнительной учебной литературы, Интернет-ресурсов, необходимых для освоения дисциплины**

Основная литература

1. Информационная безопасность : практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2019. - 84 с. - ISBN 978-5-91612-276-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1094244 (дата обращения: 11.03.2022). – Режим доступа: по подписке.

2. 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: 11.03.2022). – Режим доступа: по подписке.

3. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2022. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1862651 (дата обращения: 11.03.2022). – Режим доступа: по подписке.

Дополнительная литература

1. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 223 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5cc15bb22f5345.11209330. - ISBN 978-5-16-014397-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189349 (дата обращения: 11.03.2022). – Режим доступа: по подписке.

2. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности : учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2022. — 236 с. - ISBN 978-5-369-01788-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843171 (дата обращения: 11.03.2022). – Режим доступа: по подписке.

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:// biblioclub.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. 6. Информатика. Программа для основной школы: 8–9 классы, авторы Семакин И. Г.

и др.– Режим доступа: http://metodist.lbz.ru/ authors/informatika/2/

7. Коллекция цифровых образовательных ресурсов (ЦОР) к учебникам информатики.

Режим доступа: http://school-collection.edu.ru/

8. Преподавание, наука и жизнь: сайт Константина Полякова Режим доступа: http://kpolyakov.narod.ru/school/probook/prakt.htm

9. Журнал Информатика – Режим доступа: http://inf.1september.ru/

10. Журнал Информатика в школе – Режим доступа: http://infojournal.ru/journal/school/

11. Журнал Информатика и образование – Режим доступа: http://infojournal.ru/journal/info/