МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

РАБОЧАЯ ПРОГРАММА

Шифр	Наименование дисциплины (модуля)
Б1.В.ДВ	**Аппаратно-программное обеспечение ИБ**

Код направления подготовки	44.03.04
Направление подготовки	Профессиональное обучение (по отраслям)
Наименование (я) ОПОП (направленность / профиль)	Информатика и вычислительная техника
Уровень образования	бакалавр
Форма обучения	очная

Разработчики:

Должность	Учёная степень, звание	Подпись	ФИО
Старший преподаватель	кандидат педагогических наук		Гафарова Елена Аркадьевна

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

Кафедра	Заведующий кафедрой	Номер протокола	Дата протокола	Подпись
Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	10	13.06.2019	
Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	1	13.09.2020	

ОГЛАВЛЕНИЕ

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Дисциплина «Аппаратно-программное обеспечение ИБ» относится к модулю части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы по направлению подготовки 44.03.04 «Профессиональное обучение (по отраслям)» (уровень образования бакалавр). Дисциплина является дисциплиной по выбору.

1.2 Общая трудоемкость дисциплины составляет 2 з.е., 72 час.

1.3 Изучение дисциплины «Аппаратно-программное обеспечение ИБ» основано на знаниях, умениях и навыках, полученных при изучении обучающимися следующих дисциплин: «Администрирование информационных систем», «Аппаратные средства вычислительной техники», «Безопасность жизнедеятельности», «Информатика», «Основы информационной безопасности», «Правоведение».

1.4 Дисциплина «Аппаратно-программное обеспечение ИБ» формирует знания, умения и компетенции, необходимые для освоения следующих дисциплин: «Информационное право», «Криптографические методы защиты информации», «Цифровое образование».

1.5 Цель изучения дисциплины:

формирование у студентов системы теоретических знаний и практических навыков, необходимых для совершенствования управления информационной безопасностью в аспекте применения программно-аппаратных средств

1.6 Задачи дисциплины:

1) дать студентам знания сущность информационной безопасности, правовые нормы, регламентирующие ее реализацию;
понятие и современное состояние средств информационной защиты;
понятие семиуровневой системы обеспечения информационной безопасности;
компоненты программно-аппаратных средств обеспечения информационной защиты;системы оценки информационной защищенности

2) научить студентов давать оценку защищенности информационной системе;
применять на практике программно-аппаратные средства ОИБ

3) научить выстраивать комплексную систему защиты информации по принципу разумной достаточности

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

№ п/п	Код и наименование компетенции по ФГОС
	Код и наименование индикатора достижения компетенции
1	ПК-6 способен подбирать методы предпроектного анализа для решения поставленной задачи, методы проектирования необходимого отраслевого обеспечения для решения профессиональных задач
	ПК.6.1 Знать методы предпроектного анализа для решения поставленной задачи.
	ПК.6.2 Уметь подбирать методы предпроектного анализа для решения поставленной задачи.
	ПК.6.3 Владеть методами предпроектного анализа для решения поставленной задачи.

№ п/п	Код и наименование индикатора достижения компетенции	Образовательные результаты по дисциплине
1	ПК.6.1 Знать методы предпроектного анализа для решения поставленной задачи.	З.1 Знает научные тенденции отечественных и зарубежных исследований перспективных технологий применения инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности
2	ПК.6.2 Уметь подбирать методы предпроектного анализа для решения поставленной задачи.	У.1 Умеет применять перспективные технологические разработки инженерно-технических и программно-аппаратных средств обеспечения информационной безопасности в практике
3	ПК.6.3 Владеть методами предпроектного анализа для решения поставленной задачи.	В.1 Владеет научными основами практики применения перспективных технологические разработки инженер-но-технических и программно-аппаратных средств обеспечения информационной безопасности

2. ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДОВ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Наименование раздела дисциплины (темы)	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Итого часов
	Л	ЛЗ	ПЗ	СРС	
Итого по дисциплине	**12**	**6**	**14**	**40**	**72**
Первый период контроля					
Основные средства и методы программно-аппаратной защиты информации.	***2***	***2***		***8***	***12***
Основные средства и методы программно-аппаратной защиты информации.	2			4	6
Установление пароля на текстовый документ, архивирование документов и установление пароля на архив, установление пароля на папку		2		4	6
Идентификация, аутентификация. Управление доступом.	***2***	***4***	***6***	***12***	***24***
Аутентификация и идентификация – основной сервис ИБ	2		2	4	8
Назначение прав пользователей при произвольном управлении доступом.		2	2	4	8
Изучение настроек Ethernet и способов администрирования на сетевых интерфейсах в ОС Windows.		2	2	4	8
Протоколирование и аудит. Анализ защищенности.	***4***		***4***	***8***	***16***
Протоколирование и аудит	2		2	4	8
Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств.	2		2	4	8
Экранирование. Классификация межсетевых экранов	***4***		***4***	***12***	***20***
Классификация сетевых экранов	2		2	4	8
Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях	2		2	4	8
Анитивирусное ПО				4	4
Итого по видам учебной работы	12	6	14	40	72
Форма промежуточной аттестации					
Зачет					
Итого за Первый период контроля					**72**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

3.1 Лекции

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Основные средства и методы программно-аппаратной защиты информации.	***2***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	
1.1. Основные средства и методы программно-аппаратной защиты информации. Основные средства и методы программно-аппаратной защиты информации. 2 1. Обзор современных средств защиты информации 2. Классы сервисов ИБ 3. ГОСТы и стандарты в области ИБ Учебно-методическая литература: 1, 2	2
2. Идентификация, аутентификация. Управление доступом.	***2***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	
2.1. Аутентификация и идентификация – основной сервис ИБ Аутентификация и идентификация – основной сервис ИБ 1. Парольная аутентификация, наложение технических ограничений на пароли. 2. Одноразовые и односторонние пароли. 3. Принцип действия сервера аутентификации. 4. Биометрическая идентификация и аутентификация. 5. Матрица доступа. Ролевой доступ. 6. Объектно-ориентированный подход в администрировании ролевого доступа. Учебно-методическая литература: 1, 2, 3, 4	2
3. Протоколирование и аудит. Анализ защищенности.	***4***
Формируемые компетенции, образовательные результаты: ПК-6: У.1 (ПК.6.2)	
3.1. Протоколирование и аудит Протоколирование и аудит. 1. Общие сведения о нарушении доступа к дисковой и оперативной памяти. 2. Диагностирование и устранение логических и физических дефектов носителей информации. 3. Защита файлов от удаления и восстановление удаленных файлов. Ручное восстановление данных. Безопасное окончание работы на компьютере Учебно-методическая литература: 1, 4, 5	2
3.2. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств. 1. Основные способы защиты от потери информации и нарушений работоспособности. вычислительных средств. 2. Способы резервирования информации. 3. Правила обновления резервных данных. 4. Методы сжатия информации. 5. Архивация файловых данных. 6. Безопасная инсталляция программных средств. Учебно-методическая литература: 1, 3, 5	2
4. Экранирование. Классификация межсетевых экранов	***4***
Формируемые компетенции, образовательные результаты: ПК-6: В.1 (ПК.6.3)	

4.1. Классификация сетевых экранов Классификация сетевых экранов 1. Поддержание целостности циркулирующих в сети сообщений. 2.Формирование и проверка цифровой подписи. 3. Защита от отрицания фактов отправки и приема сообщений. 4.Типы межсетевых экранов, их достоинства и недостатки Учебно-методическая литература: 1, 3, 5 Профессиональные базы данных и информационные справочные системы: 1	2
4.2. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях Лабораторная работа: Использование межсетевых экранов (брандмауэров) для защиты информации в сетях Цель работы:овладеть навыками работы с сетевой программой ATGuard. Теоретические сведения. Требования к установке:Операционная система: Windows 95, Windows 98, WindowsNT 4.0 + ServicePack 3, Windows 2000 и выше. Неподдерживаются: Windows NT 3.51, Windows 3.1x, Windows ME, Mac, Linux/UNIX. Компьютер: на Intel 80386DX или выше (для Windows 95), или на 486/25 или выше (для Windows NT 4.0). Около 3 MB свободного дискового пространства. Установленный протокол TCP/IP. Общие сведения о межсетевых экранах. Межсетевой экран(firewall или брандмауэр) является программно-аппаратным средством осуществления сетевой политики безопасности в выделенном сегменте IP-сети. В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от вторжения злоумышленников во внутреннюю локальную сеть для того, чтобы скопировать, изменить или стереть информацию либо воспользоваться памятью или вычислительной мощностью работающих в этой сети компьютеров. Межсетевой экран призван обеспечить безопасный доступ к внешней сети и ограничить доступ внешних пользователей к внутренней сети Учебно-методическая литература: 3, 5 Профессиональные базы данных и информационные справочные системы: 1	2

3.2 Лабораторные

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Основные средства и методы программно-аппаратной защиты информации.	***2***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	
1.1. Установление пароля на текстовый документ, архивирование документов и установление пароля на архив, установление пароля на папку Установление пароля на текстовый документ, архивирование документов и установление пароля на архив, установление пароля на папку. 1. Установление пароля на текстовый документ 2. архивирование документов 3. установление пароля на архив 4. установление пароля на папку. Учебно-методическая литература: 2, 3	2
2. Идентификация, аутентификация. Управление доступом.	***4***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	

2.1. Назначение прав пользователей при произвольном управлении доступом. Назначение прав пользователей при произвольном управлении доступом. 1. Пользователи ИС и их атрибуты 2. Назначение прав пользователей. 3. Реализация прав доступа Учебно-методическая литература: 3, 4 Профессиональные базы данных и информационные справочные системы: 1	2
2.2. Изучение настроек Ethernet и способов администрирования на сетевых интерфейсах в ОС Windows. Изучение настроек Ethernet и способов администрирования на сетевых интерфейсах в ОС Windows. 1. Ознакомление с интерфейсом и функционалом Ethernet 2. Способы администрирования ОС 3. Реализация администрирования через Ethernet Учебно-методическая литература: 3	2

3.3 Практические

Наименование раздела дисциплины (модуля)/ Тема и содержание	**Трудоемкость (кол-во часов)**
1. Идентификация, аутентификация. Управление доступом.	***6***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	
1.1. Аутентификация и идентификация – основной сервис ИБ Аутентификация и идентификация – основной сервис ИБ 1. Парольная аутентификация, наложение технических ограничений на пароли. 2. Одноразовые и односторонние пароли. 3. Принцип действия сервера аутентификации. 4. Биометрическая идентификация и аутентификация. 5. Матрица доступа. Ролевой доступ. 6. Объектно-ориентированный подход в администрировании ролевого доступа. Учебно-методическая литература: 3, 5	2
1.2. Назначение прав пользователей при произвольном управлении доступом. Назначение прав пользователей при произвольном управлении доступом. 1. Пользователи ИС и их атрибуты 2. Назначение прав пользователей. 3. Реализация прав доступа Учебно-методическая литература: 3, 4 Профессиональные базы данных и информационные справочные системы: 1	2
1.3. Изучение настроек Ethernet и способов администрирования на сетевых интерфейсах в ОС Windows. Изучение настроек Ethernet и способов администрирования на сетевых интерфейсах в ОС Windows. 1. Ознакомление с интерфейсом и функционалом Ethernet 2. Способы администрирования ОС 3. Реализация администрирования через Ethernet Учебно-методическая литература: 3, 5 Профессиональные базы данных и информационные справочные системы: 1	2
2. Протоколирование и аудит. Анализ защищенности.	***4***
Формируемые компетенции, образовательные результаты: ПК-6: У.1 (ПК.6.2)	
2.1. Протоколирование и аудит Протоколирование и аудит. 1. Общие сведения о нарушении доступа к дисковой и оперативной памяти. 2. Диагностирование и устранение логических и физических дефектов носителей информации. 3. Защита файлов от удаления и восстановление удаленных файлов. Ручное восстановление данных. Безопасное окончание работы на компьютере. Учебно-методическая литература: 1, 2, 4	2

2.2. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств. 1. Основные способы защиты от потери информации и нарушений работоспособности. вычислительных средств. 2. Способы резервирования информации. 3. Правила обновления резервных данных. 4. Методы сжатия информации. 5. Архивация файловых данных. 6. Безопасная инсталляция программных средств. Учебно-методическая литература: 2, 3, 5	2
3. Экранирование. Классификация межсетевых экранов	***4***
Формируемые компетенции, образовательные результаты: ПК-6: В.1 (ПК.6.3)	
3.1. Классификация сетевых экранов . Классификация сетевых экранов 1. Поддержание целостности циркулирующих в сети сообщений. 2.Формирование и проверка цифровой подписи. 3. Защита от отрицания фактов отправки и приема сообщений. 4.Типы межсетевых экранов, их достоинства и недостатки Учебно-методическая литература: 2, 3, 5 Профессиональные базы данных и информационные справочные системы: 2	2

3.2. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях	2

Лабораторная работа: Использование межсетевых экранов (брандмауэров) для защиты информации в сетях
Цель работы:овладеть навыками работы с сетевой программой ATGuard.
Теоретические сведения.
Требования к установке:Операционная система: Windows 95, Windows 98, WindowsNT 4.0 + ServicePack 3, Windows 2000 и выше. Неподдерживаются: Windows NT 3.51, Windows 3.1x, Windows ME, Mac, Linux/UNIX.
Компьютер: на Intel 80386DX или выше (для Windows 95), или на 486/25 или выше (для Windows NT 4.0).
Около 3 MB свободного дискового пространства.
Установленный протокол TCP/IP.
Общие сведения о межсетевых экранах.
Межсетевой экран(firewall или брандмауэр) является программно-аппаратным средством осуществления сетевой политики безопасности в выделенном сегменте IP-сети.
В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от вторжения злоумышленников во внутреннюю локальную сеть для того, чтобы скопировать, изменить или стереть информацию либо воспользоваться памятью или вычислительной мощностью работающих в этой сети компьютеров.
Межсетевой экран призван обеспечить безопасный доступ к внешней сети и ограничить доступ внешних пользователей к внутренней сети (см. рис 1.)
Рис 1. Схема установления firewall.
Название «брандмауэр», может относиться к одному устройству или од¬ной программе. Термин «межсетевой экран» был принят для обозначения совокупности компонен¬тов, которые находятся между вашей сетью и внешним миром и образуют защит¬ный барьер.
Брандмауэр не может защитить от:
 вирусов.Хотя некоторые брандмауэры и способны распознавать вирусы в про-ходящем через них трафике, существует множество способов спрятать вирусы в программе. Если даже в описании вашего брандмауэра заявлена функция антивирусной проверки, не выключайте проверку вирусов на отдельных ком-пьютерах в сети;
 «троянских коней». Как и в случае с вирусами, блокировать проникновение в сеть «троянских коней» (Trojanhorses) достаточно сложно. Пользователь нередко поддается искушению загрузить программу из Internet или открыть прикрепленный к сообщению электронной почты файл, проложив тем самым путь в систему вредоносной программе;
 «социальной инженерии». Термин «socialengineering» возник недавно и при-меняется для описания методов получения хакерами информации от довер¬чивых пользователей. Часто люди готовы сообщить свой пароль любому, кто позвонил по телефону и отреко¬мендовался представителем службы безопасности, что-нибудь «проверяю¬щим». Межсетевой экран не в состоянии остановить невоздержного на язык сотрудника
 некомпетентности. Плохо подготовленные сотрудники или небрежное руко-водство приводят к ошибкам в настройках локальной сети и межсетевого экрана. Если сотрудники не понимают, как работает брандмауэр и как пра¬вильно его настраивать, не исключено, что это будет способствовать возник¬новению проблем;
 атаки изнутри. Межсетевой экран не может предотвратить злонамеренные дей-ствия внутри вашей сети. Это одна из причин, покоторой безопасность компью-теров в сети остается важной проблемой и после установки брандмауэра.
Интерфейс AtGuard.
После инсталляции программы и перезагрузки компьютера Вы обнаружите в системном трее (system tray) иконку запущенного AtGuard’a , а вверху экрана его же панель (dashboard)
Рис 2. Внешний вид dashboard
Это означает, что инсталляция и первый запуск прошли успешно. Двойной щелчок на иконке открывает окно настроек.
AtGuard Settings / Web
Рис 3. Окно настроек Web
Установка флажка Enable web filters включает блокирование, опции секретности и активные установки фильтров, определенные в диалоговом окне Web (HTTP) Filters. Уберите этот флажок, если Вы хотите выключить все web-фильтры.
Enable web filters действует как главный переключатель, который позволяет вам отменять индивидуальные установки фильтра в диалоговом окне Web (HTTP) Filters и отключать всю фильтрацию веб-трафика
Учебно-методическая литература: 3, 5
Профессиональные базы данных и информационные справочные системы: 2

3.4 СРС

Наименование раздела дисциплины (модуля)/ Тема для самостоятельного изучения	**Трудоемкость (кол-во часов)**
1. Основные средства и методы программно-аппаратной защиты информации.	***8***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	
1.1. Основные средства и методы программно-аппаратной защиты информации. ***Задание для самостоятельного выполнения студентом:*** Основные средства и методы программно-аппаратной защиты информации. 1. Обзор современных средств защиты информации 2. Классы сервисов ИБ 3. ГОСТы и стандарты в области ИБ Учебно-методическая литература: 2, 3	4
1.2. Установление пароля на текстовый документ, архивирование документов и установление пароля на архив, установление пароля на папку ***Задание для самостоятельного выполнения студентом:*** Установление пароля на текстовый документ, архивирование документов и установление пароля на архив, установление пароля на папку. 1. Установление пароля на текстовый документ 2. архивирование документов 3. установление пароля на архив 4. установление пароля на папку. Учебно-методическая литература: 1, 3, 5	4
2. Идентификация, аутентификация. Управление доступом.	***12***
Формируемые компетенции, образовательные результаты: ПК-6: З.1 (ПК.6.1)	
2.1. Аутентификация и идентификация – основной сервис ИБ ***Задание для самостоятельного выполнения студентом:*** Аутентификация и идентификация – основной сервис ИБ 1. Парольная аутентификация, наложение технических ограничений на пароли. 2. Одноразовые и односторонние пароли. 3. Принцип действия сервера аутентификации. 4. Биометрическая идентификация и аутентификация. 5. Матрица доступа. Ролевой доступ. 6. Объектно-ориентированный подход в администрировании ролевого доступа Учебно-методическая литература: 1, 3, 5	4
2.2. Назначение прав пользователей при произвольном управлении доступом. ***Задание для самостоятельного выполнения студентом:*** Назначение прав пользователей при произвольном управлении доступом. 1. Пользователи ИС и их атрибуты 2. Назначение прав пользователей. 3. Реализация прав доступа Учебно-методическая литература: 3, 5	4
2.3. Изучение настроек Ethernet и способов администрирования на сетевых интерфейсах в ОС Windows. ***Задание для самостоятельного выполнения студентом:*** Изучение настроек Ethernet и способов администрирования на сетевых интерфейсах в ОС Windows. 1. Ознакомление с интерфейсом и функционалом Ethernet 2. Способы администрирования ОС 3. Реализация администрирования через Ethernet Учебно-методическая литература: 2, 5	4
3. Протоколирование и аудит. Анализ защищенности.	***8***
Формируемые компетенции, образовательные результаты: ПК-6: У.1 (ПК.6.2)	

3.1. Протоколирование и аудит ***Задание для самостоятельного выполнения студентом:*** Протоколирование и аудит. 1. Общие сведения о нарушении доступа к дисковой и оперативной памяти. 2. Диагностирование и устранение логических и физических дефектов носителей информации. 3. Защита файлов от удаления и восстановление удаленных файлов. Ручное восстановление данных. Безопасное окончание работы на компьютере. Учебно-методическая литература: 3, 5	4
3.2. Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств. ***Задание для самостоятельного выполнения студентом:*** Анализ защищенности. Защита от потери информации и отказов программно-аппаратных средств. 1. Основные способы защиты от потери информации и нарушений работоспособности. вычислительных средств. 2. Способы резервирования информации. 3. Правила обновления резервных данных. 4. Методы сжатия информации. 5. Архивация файловых данных. 6. Безопасная инсталляция программных средств Учебно-методическая литература: 2, 3	4
4. Экранирование. Классификация межсетевых экранов	***12***
Формируемые компетенции, образовательные результаты: ПК-6: В.1 (ПК.6.3)	
4.1. Классификация сетевых экранов ***Задание для самостоятельного выполнения студентом:*** Классификация сетевых экранов 1. Поддержание целостности циркулирующих в сети сообщений. 2.Формирование и проверка цифровой подписи. 3. Защита от отрицания фактов отправки и приема сообщений. 4.Типы межсетевых экранов, их достоинства и недостатки Учебно-методическая литература: 1, 4, 5	4

4.2.	Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях ***Задание для самостоятельного выполнения студентом:*** Add Firewall Rule Name. Это просто краткое описание вашего правила. Имя правила также появится в Firewall лог-файле, если вы выберете регистрацию события для этого правила. Рис 5. Окно Add firewall rule Action. Permit (разрешить), Block (запретить), Ignore (игнорировать). Регистрирует событие в лог-файле. Затем обработка события продолжается, пока не будет найдено соответствующее правило. Если никакое правило не будет найдено связь или блокируется (по умолчанию) или вызывается RuleAssistant. Как использовать правило Ignore?Когда задано правило Ignore, происходит регистрация события и затем обработка продолжается пока не будет найдено правило разрешающее или запрещающее данный тип связи. Обратите внимание: для того чтобы правило Ignore сработало, оно должно появиться в списке правил firewall'a выше любого правила описывающего данный тип связи. Лучше поместить все правила Ignore в верхнюю часть списка firewall. Действие Ignore предназначено, чтобы позволить Вам регистрировать события до предписания "Разрешить" или "Блокировать", которое применяется к этому типу связи. Например, есть разрешающее правило firewall, которое позволяет вашему FTP серверу связываться с любым сетевым адресом. Можно отследить, как часто пользователи с определенного сетевого адреса соединялись с вашим FTP сервером, задав игнорирующее правило для регистрации соединений. Правило Ignore должно предшествовать правилу Permit. Direction. Inbound связь включает пакеты, посланные вашему компьютеру. Outbound связь включает пакеты, посланные вашим компьютером. Either - связь в любом направлении. Protocol. Определяет, к какому протоколу связи применяется правило: TCP, UDP, или TCP и UDP, ICMP... TCP - стандартный протокол Интернета транспортного уровня, обеспечивает надежную полнодуплексную связь. Программное обеспечение, реализующее протокол TCP, обычно постоянно находится в операционной системе и использует IP протокол, чтобы передать информацию. Примеры TCP приложений и сервисов - FTP, web-браузер, email и IRC. UDP - транспортый уровень в TCP/IP сетях. UDP - низкоуровневый протокол, который использует IP, чтобы доставить пакеты. Примеры сервисов и приложений, которые используют UDP - DNS, NetBIOS. ICMP - протокол межсетевых управляющих сообщений. Application. Эта опция позволяет определять, применяется ли правило к конкретному приложению или к любому приложению, которое делает попытку сетевой связи, определенной правилом. Service. Позволяет определять, применяется ли правило к локальным или удаленным сервисам и применяется ли это к одиночному определенному сервису или к любому сервису, который делает попытку сетевой связи, определенной правилом. Сервисы - протоколы, которые используются, чтобы позволить одному компьютеру обращаться к специфическому виду данных, сохраненных в другом компьютере. Например, HTTP серверы используют протокол передачи гипертекста, чтобы обеспечить по всему миру сервис web, FTP серверы предлагают сервисы протокола передачи файла, SMTP серверы используют простой протокол транспорта почты, чтобы посылать почту, и POP серверы используют POP протокол, чтобы передать электронную почту. Учебно-методическая литература: 3, 4, 5	4
4.3.	Анитивирусное ПО ***Задание для самостоятельного выполнения студентом:*** Установка антивирусного ПО. Сканирование внешнего носителя на наличие вирусов 1.История появления компьютерных вирусов и факторы, влияющие на их распространение. 2.Понятие компьютерного вируса. 3.Основные этапы жизненного цикла вирусов. 4. Объекты внедрения, режимы функционирования и специальные функции вирусов. 5.Схемы заражения файлов. 6.Классификация компьютерных вирусов. Учебно-методическая литература: 3 Профессиональные базы данных и информационные справочные системы: 1	4

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Ссылка на источник в ЭБС
	Основная литература	
1	Прокушев Я.Е. Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие/ Прокушев Я.Е.— Электрон. текстовые данные.— Санкт-Петербург: Интермедия, 2017.— 160 c.	Режим доступа: http://www.iprbookshop.ru/66799.html.— ЭБС «IPRbooks»
2	Программно-аппаратные средства защиты информации [Электронный ресурс]: учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность»/ Л.Х. Мифтахова [и др.].— Электрон. текстовые данные.— Санкт-Петербург: Интермедия, 2018.— 408 c.	Режим доступа: http://www.iprbookshop.ru/73644.html.— ЭБС «IPRbooks»
3	Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс]/ — Электрон. текстовые данные.— Москва: Московский технический университет связи и информатики, 2016.— 31 c.	Режим доступа: http://www.iprbookshop.ru/61529.html.— ЭБС «IPRbooks»
	Дополнительная литература	
4	Костин В.Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации [Электронный ресурс]: учебное пособие/ Костин В.Н.— Электрон. текстовые данные.— Москва: Издательский Дом МИСиС, 2018.— 21 c.	Режим доступа: http://www.iprbookshop.ru/98199.html.— ЭБС «IPRbooks»
5	Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс]: научно-техническое издание/ А.И. Астайкин [и др.].— Электрон. текстовые данные.— Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015.— 224 c.	Режим доступа: http://www.iprbookshop.ru/60959.html.— ЭБС «IPRbooks»

4.2. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

№ п/п	Наименование базы данных	Ссылка на ресурс
1	Единое окно доступа к образовательным ресурсам	http://window.edu.ru
2	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

5.1. Описание показателей и критериев оценивания компетенций

Код компетенции по ФГОС					
Код образовательного результата дисциплины	Текущий контроль				Промежуточная аттестация
	Кейс-задачи	Опрос	Тест	Эссе	Зачет/Экзамен
ПК-6					
З.1 (ПК.6.1)		+	+		+
У.1 (ПК.6.2)	+				+
В.1 (ПК.6.3)				+	+

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

5.2.1. Текущий контроль.

Типовые задания к разделу "Основные средства и методы программно-аппаратной защиты информации.":

1. Опрос

1. Что такое ATGuard и для чего применяется?
2. От чего защищает и от чего не защищает ATGuard?
3. Как ATGuard вырезает баннеры и активное содержимое?
4. Зачем скрывать информацию о cookies файлах?
5. Как можно избирательно устанавливать настройки для определенных сайтов?
6. Как посмотреть статистику и лог-файлы?
7. Как работает ATGuard с прокси-серверами?

Количество баллов: 5

Типовые задания к разделу "Идентификация, аутентификация. Управление доступом.":

1. Тест

1. Выберите все правильные варианты ответов
Активным видом атак является
 отказ в обслуживании - DoS-атака (Denial of Service)
 модификация потока данных - атака "man in the middle"
 фальсификация (нарушение аутентичности) - попытка одного субъекта выдать себя за другого
 прослушивание (сниффинг)
 анализ трафика
2. Выберите все правильные варианты ответов
Алгоритм симметричного шифрования может быть применим в
 шифровании большого потока данных
 создании определенного количества случайных битов
 хэшировании данных
 секретной передаче ключа
3. Выберите все правильные варианты ответов
Односторонняя функция с секретом - это
 односторонняя функция, которую легко вычислить в одном направлении и трудно вычислить в обратном направлении до тех пор, пока недоступна некоторая дополнительная информация
 при наличии дополнительной информации инверсию можно вычислить за полиномиальное время
 при наличии дополнительной информации инверсию можно вычислить за экспоненциальное время
4 Выберите все правильные варианты ответов
Укажите основные угрозы информационной безопасности в вычислительных сетях
 несанкционированный доступ к информации
 искажение информации или подлог (имитация)
 отказ от авторства
 отказ от шифрования
 взлом сейфа с ценными бумагами
5. Выберите все правильные варианты ответов
В необходимый минимум средств защиты от вирусов входит:
 архивирование
 профилактика
 входной контроль

Количество баллов: 5

Типовые задания к разделу "Протоколирование и аудит. Анализ защищенности.":

1. Кейс-задачи

Задача 1: У менеджера компании есть личный электронный ящик, также что она пользуется социальными сетями (Вконтакте, Одноклассники, КрасМама и пр). При этом она закрывает браузер не нажимая кнопку "выход", использует Internet Explorer, имеет 1-2 несложных пароля на все ресурсы, выходит в сеть в основном с рабочего места иногда из дома. Девушка коммуникабельная, активная участница форумов. На сайтах регестрируется под ником ***
Студенты делятся на 2 группы: "Защитники" (Админы) и "Злоумышленники" (Хакеры),
Каждая команда сообразно своим интересам определяет для менеджера:
• Риски по аспектам информационной безопасности: целостность, доступность, конфиденциальность
• Уязвимости
• Угрозы
• Уровень неприемлемого ущерба
• Контрмеры - политику безопасности (для защитников)
• Порядок атак (для злоумышленников)
После обсуждения, студентам сообщается имя девушки и её ник (он виртуальный). Студенты выходят в Интернет, и кто первый успеет (найти почту, поменять пароли, сменить данные, чтоб не нашли другие и пр), тот и победил.

Количество баллов: 5

Типовые задания к разделу "Экранирование. Классификация межсетевых экранов":

1. Эссе

Образец эссе.

Классификации современных программно-аппаратных комплексов

Бурное развитие средств вычислительной техники, автоматизированных информационных систем, появление новых информационных технологий в нашей стране сопровождается появлением таких малоприятных явлений, как промышленный шпионаж, компьютерная преступность и прежде всего несанкционированный доступ к конфиденциальной информации. Этим обуславливается актуальность и значимость проблемы защиты информации. Острая необходимость в защите информации нашла выражение в создании Государственной системы защиты информации (ГСЗИ). Развивается так же и правовая база информационной безопасности, а именно, приняты и введены в действие законы «О государственной тайне», «Об информации, информатизации и защите информации», «О правовой охране программ для электронных вычислительных машин и баз данных» и др. Целями защиты информации являются:

1. предотвращение ущерба, возникновение которого возможно в результате утери (хищения, утраты, искажения, подделки) информации в любом ее проявлении;
2. реализация адекватных угрозам безопасности информации мер защиты в соответствии с действующими законами и нормативными документами по безопасности информации
3. создание определенных программно-аппаратных средств защиты, соответствующих потребностям владельцев (пользователей) информации.

Любое современное предприятие (учреждение, фирма и т.д.), независимо от вида деятельности и форм собственности, не может сегодня успешно развиваться и вести хозяйственную и иную деятельность без создания надежной системы защиты своей информации, включающей не только организационно-нормативные меры, но и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах, прежде всего, программно-аппаратные.

Большинство функций современных КС реализованы в виде программ, поддержание целостности которых при запуске системы и особенно в процессе функционирования является трудной задачей. Значительное число пользователей в той или иной степени обладают познаниями в программировании, осведомлены об ошибках в построении операционных систем. Поэтому существует достаточно высокая вероятность применения ими имеющихся знаний для атак на программное обеспечение. Проверка целостности одних программ при помощи других не является надежной. Необходимо четко представлять, каким образом обеспечивается целостность собственно программы проверки целостности. Если обе программы находятся на одних и тех же носителях, доверять результатам такой проверки нельзя. В связи с этим к программным системам защиты от несанкционированного доступа следует относиться с особой осторожностью.

Использование аппаратных средств снимает проблему обеспечения целостности системы. В большинстве современных систем защиты от НСД применяется зашивка программного обеспечения в ПЗУ или в аналогичную микросхему. Таким образом, для внесения изменений вПО необходимо получить доступ к соответствующей плате и заменить микросхему. В случае использования универсального процессора реализация подобных действий потребует применения специального оборудования, что еще более затруднит проведение атаки. Использование специализированного процессора с реализацией алгоритма работы в виде интегральной микросхемы полностью снимает проблему нарушения целостности этого алгоритма.

Для того, чтобы защитить информацию от НСД, существует ряд специально проводимых мер:

• Применение аппаратных средств:
о установка фильтров, межсетевых экранов;
о блокировка клавиатуры;
о устройства аутентификации;
о использование электронных замков на микросхемах.
• Применение программных средств:
о использование пароля для доступа к компьютеру;
о использование средств парольной защиты BIOS — как на сам BIOS, так и на ПК в целом.
• Применение аппаратно-программных средств:
о использование аппаратно-программных средств доверенной загрузки
• Применение шифрования:
о Шифрование — это преобразование (кодирование) открытой информации в зашифрованную, для передачи закрытой информации или сведений, составляющих государственную тайну информации по незащищенным каналам связи. Зачастую, сам алгоритм шифрования известен всем, а ключ, с помощью которого можно расшифровать данное сообщение засекречен.
• Проведение организационных мероприятий:
о осуществление пропускного режима;
о хранение носителей информации в закрытом доступе;
о ограничение лиц, имеющих доступ к компьютеру.

Количество баллов: 5

5.2.2. Промежуточная аттестация

Промежуточная аттестация проводится в соответствии с Положением о текущем контроле и промежуточной аттестации в ФГБОУ ВО «ЮУрГГПУ».

Первый период контроля

1. Зачет

Вопросы к зачету:

1. • Защита авторских прав на электронные документы в России. Правовая база.
2. • Применение электронной подписи (ЭП) в России (хранение ЭП, идентификация и аутентификация при помощи ЭП).
3. • Правовая база применения ЭП в России.
4. • Защищенные централизованные хранилища данных (ЦХД): принципы построения, продукты-менеджеры, угрозы ЦХД.
5. • Утечка информации при помощи побочного электромагнитного излучения и наводок (ПЭМИН).
6. • Стандарт ISO/IEC 17799:2005.
7. • Стандарт ISO/IEC 27001:2005.
8. • Стандарт BS 7799-3:2006.
9. • Обзор новых и широко используемых криптографических стандартов и алгоритмов.
10. • Обзор современных программных средств криптографического управления данными (шифрование, удаление, создание защищенных дисков и т.д.).
11. • Протоколы шифрования при передаче по сети (в т.ч. беспроводной). Примеры (WPA и т.д.)
12. • Обзор программных средств выполнения активного аудита.
13. • Защита от копирования CD, DVD дисков.
14. • Целостность информации. Средства резервного копирования. Обзор имеющихся средств.
15. • Средства восстановления потерянных или удаленных файлов. Средства полного уничтожения информации.
16. • Виртуальные машины. Примеры. Работа с VMWare.
17. • Методы и средства идентификации и аутентификации в компьютерных системах.
18. • Устройство и работа бесконтактных карт, смарт-карт, электронных ключей и т.п.
19. • Наиболее известные и удачные попытки взлома последних двух лет.
20. • Классификация вредоносных программ. Методы защиты, алгоритмы работы противоборствующих программ.
21. • Принцип работы программных и аппаратных межсетевых экранов (МЭ). Предлагаемые возможности.
22. • Решения по защите от несанкционированного использования мобильных устройств (мобильных телефонов, смартфонов, КПК и т.п.)
23. • Защита Web-сервера. Организация доступа к Web-серверу для просмотра информации.
24. • Возможность удаленного управления компьютером (УУК). Защита от несанкционированного УУК.
25. • Обзор локальных и сетевых программ-шпионов (клавиатурные, запуск программ, клавиатурные в окне конкретной программы и т.п.).
26. • Программные средства по контролю за действиями пользователей
27. • Защита от перехвата трафика, передаваемого по радиоканалам (wi-fi, bluetooth, и т.д.), защита точек доступа, построение беспроводных сетей.
28. • Организация и защита VPN-сетей. Безопасность VoIP.

5.3. Примерные критерии оценивания ответа студентов на экзамене (зачете):

Отметка	Критерии оценивания
"Отлично"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - умение обоснованно излагать свои мысли, делать необходимые выводы
"Хорошо"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя - умение обоснованно излагать свои мысли, делать необходимые выводы

"Удовлетворительно" ("зачтено")	- затруднения с комплексной оценкой предложенной ситуации - неполное теоретическое обоснование, требующее наводящих вопросов преподавателя - выполнение заданий при подсказке преподавателя - затруднения в формулировке выводов
"Неудовлетворительно" ("не зачтено")	- неправильная оценка предложенной ситуации - отсутствие теоретического обоснования выполнения заданий

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Лекции

Лекция - одна из основных форм организации учебного процесса, представляющая собой устное, монологическое, систематическое, последовательное изложение преподавателем учебного материала с демонстрацией слайдов и фильмов. Работа обучающихся на лекции включает в себя: составление или слежение за планом чтения лекции, написание конспекта лекции, дополнение конспекта рекомендованной литературой.

Требования к конспекту лекций: краткость, схематичность, последовательная фиксация основных положений, выводов, формулировок, обобщений. В конспекте нужно помечать важные мысли, выделять ключевые слова, термины. Последующая работа над материалом лекции предусматривает проверку терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. В конспекте нужно обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

2. Лабораторные

Лабораторные занятия проводятся в специально оборудованных лабораториях с применением необходимых средств обучения (лабораторного оборудования, образцов, нормативных и технических документов и т.п.).

При выполнении лабораторных работ проводятся: подготовка оборудования и приборов к работе, изучение методики работы, воспроизведение изучаемого явления, измерение величин, определение соответствующих характеристик и показателей, обработка данных и их анализ, обобщение результатов. В ходе проведения работ используются план работы и таблицы для записей наблюдений.

При выполнении лабораторной работы студент ведет рабочие записи результатов измерений (испытаний), оформляет расчеты, анализирует полученные данные путем установления их соответствия нормам и/или сравнения с известными в литературе данными и/или данными других студентов. Окончательные результаты оформляются в форме заключения.

3. Практические

Практические (семинарские занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы.

Основной формой проведения практических занятий и семинаров является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

При подготовке к практическому занятию необходимо, ознакомиться с его планом; изучить соответствующие конспекты лекций, главы учебников и методических пособий, разобрать примеры, ознакомиться с дополнительной литературой (справочниками, энциклопедиями, словарями). К наиболее важным и сложным вопросам темы рекомендуется составлять конспекты ответов. Следует готовить все вопросы соответствующего занятия: необходимо уметь давать определения основным понятиям, знать основные положения теории, правила и формулы, предложенные для запоминания к каждой теме.

В ходе практического занятия надо давать конкретные, четкие ответы по существу вопросов, доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

4. Зачет

Цель зачета − проверка и оценка уровня полученных студентом специальных знаний по учебной дисциплине и соответствующих им умений и навыков, а также умения логически мыслить, аргументировать избранную научную позицию, реагировать на дополнительные вопросы, ориентироваться в массиве информации.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором обучающиеся получают предварительный перечень вопросов к зачёту и список рекомендуемой литературы, их ставят в известность относительно критериев выставления зачёта и специфике текущей и итоговой аттестации. С самого начала желательно планомерно осваивать материал, руководствуясь перечнем вопросов к зачету и списком рекомендуемой литературы, а также путём самостоятельного конспектирования материалов занятий и результатов самостоятельного изучения учебных вопросов.

По результатам сдачи зачета выставляется оценка «зачтено» или «не зачтено».

5. Опрос

Опрос представляет собой совокупность развернутых ответов студентов на вопросы, которые они заранее получают от преподавателя. Опрос может проводиться в устной и письменной форме.

Подготовка к опросу включает в себя:

- изучение конспектов лекций, раскрывающих материал, знание которого проверяется опросом;
- повторение учебного материала, полученного при подготовке к семинарским, практическим занятиям и во время их проведения;
- изучение дополнительной литературы, в которой конкретизируется содержание проверяемых знаний;
- составление в мысленной форме ответов на поставленные вопросы.

6. Тест

Тест это система стандартизированных вопросов (заданий), позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся. Тесты могут быть аудиторными и внеаудиторными. Преподаватель доводит до сведения студентов информацию о проведении теста, его форме, а также о разделе (теме) дисциплины, выносимой на тестирование.

При самостоятельной подготовке к тестированию студенту необходимо:

- проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- выяснить все условия тестирования заранее. Необходимо знать, сколько тестов вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.
- работая с тестами, внимательно и до конца прочесть вопрос и предлагаемые варианты ответов; выбрать правильные (их может быть несколько); на отдельном листке ответов выписать цифру вопроса и буквы, соответствующие правильным ответам. В случае компьютерного тестирования указать ответ в соответствующем поле (полях);
- в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.
- решить в первую очередь задания, не вызывающие трудностей, к трудному вопросу вернуться в конце.
- оставить время для проверки ответов, чтобы избежать механических ошибок.

7. Кейс-задачи

Кейс – это описание конкретной ситуации, отражающей какую-либо практическую проблему, анализ и поиск решения которой позволяет развивать у обучающихся самостоятельность мышления, способность выслушивать и учитывать альтернативную точку зрения, а также аргументировано отстаивать собственную позицию.

Рекомендации по работе с кейсом:

1. Сначала необходимо прочитать всю имеющуюся информацию, чтобы составить целостное представление о ситуации; не следует сразу анализировать эту информацию, желательно лишь выделить в ней данные, показавшиеся важными.
2. Требуется охарактеризовать ситуацию, определить ее сущность и отметить второстепенные элементы, а также сформулировать основную проблему и проблемы, ей подчиненные. Важно оценить все факты, касающиеся основной проблемы (не все факты, изложенные в ситуации, могут быть прямо связаны с ней), и попытаться установить взаимосвязь между приведенными данными.
3. Следует сформулировать критерий для проверки правильности предложенного решения, попытаться найти альтернативные способы решения, если такие существуют, и определить вариант, наиболее удовлетворяющий выбранному критерию.
4. В заключении необходимо разработать перечень практических мероприятий по реализации предложенного решения.
5. Для презентации решения кейса необходимо визуализировать решение (в виде электронной презентации, изображения на доске и пр.), а также оформить письменный отчет по кейсу.

8. Эссе

Эссе - это прозаическое сочинение небольшого объема и свободной композиции, выражающее индивидуальные впечатления и соображения по конкретному поводу или вопросу и заведомо не претендующее на определяющую или исчерпывающую трактовку предмета.

Структура эссе определяется предъявляемыми к нему требованиями: мысли автора эссе по проблеме излагаются в форме кратких тезисов; мысль должна быть подкреплена доказательствами - поэтому за тезисом следуют аргументы . При написании эссе важно также учитывать следующие моменты:

Вступление и заключение должны фокусировать внимание на проблеме (во вступлении она ставится, в заключении - резюмируется мнение автора).

Необходимо выделение абзацев, красных строк, установление логической связи абзацев: так достигается целостность работы.

Стиль изложения: эссе присущи эмоциональность, экспрессивность, художественность. Должный эффект обеспечивают короткие, простые, разнообразные по интонации предложения, умелое использование "самого современного" знака препинания - тире.

Этапы написания эссе:

1. написать вступление (2–3 предложения, которые служат для последующей формулировки проблемы).
2. сформулировать проблему, которая должна быть важна не только для автора, но и для других;
3. дать комментарии к проблеме;
4. сформулировать авторское мнение и привести аргументацию;
5. написать заключение (вывод, обобщение сказанного).

При оформлении эссе следует придерживаться рекомендаций, представленных в документе «Регламент оформления письменных работ».

7. ПЕРЕЧЕНЬ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

1. Развивающее обучение
2. Проблемное обучение
3. Кейс-технологии

8. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ

1. компьютерный класс – аудитория для самостоятельной работы
2. лаборатория
3. учебная аудитория для семинарских, практических занятий
4. Лицензионное программное обеспечение:
   - Операционная система Windows 10
   - Microsoft Office Professional Plus
   - Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition
   - Справочная правовая система Консультант плюс
   - 7-zip
   - Adobe Acrobat Reader DC