МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ И РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

«СОГЛАСОВАНО»
Руководитель ОП

_____ Сухомлинов А. И.
подпись ФИО

«УТВЕРЖДАЮ»
Директор департамента Информационных и компьютерных систем

_____ Пустовалов Е.В.
подпись ФИО
«15» июля 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность
Направление подготовки 09.03.03 Прикладная информатика
(Прикладная информатика в управлении предприятием)
Форма подготовки очная

курс 4 семестр 7
лекции 34 час.
практические занятия 00 час.
лабораторные работы 34 час.
в том числе с использованием МАО лек. 0/пр. 0/лаб. 34 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 34 час.
самостоятельная работа 40 час.
в том числе на подготовку к экзамену - час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрен
зачет 7 семестр
экзамен - семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Министерства образования и науки РФ от 19 сентября 2017 г. № 922 (с изменениями и дополнениями)

Рабочая учебная программа обсуждена на заседании кафедры информационных систем управления, протокол № 5 от «28» января 2020 г.

Директор департамента информационных и компьютерных систем Пустовалов Е.В.
Составитель: к.т.н., доцент С.Г. Фадюшин

Владивосток
2021

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании департамента:

Протокол от «17» сентября 2021 г. № 1

Директор департамента _____ Пустовалов Е.В.
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании департамента:

Протокол от «_____» _____ 20___ г. № _____

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

1. Цели и задачи освоения дисциплины:

Цель: формирование знаний теоретических основ информационной безопасности, навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи:

– формирование знаний по составу и структуре инструментальных и программных средств информационной безопасности;

– вырабатывание практических навыков по инсталлированию и эксплуатации программных компонентов информационной безопасности;

– целенаправленное воспитание по соблюдению законов и этических норм, относящихся к информационной безопасности.

Результаты освоения (формирование компетенций):

Общепрофессиональные компетенции выпускников и индикаторы их достижения:

Задача профессиональной деятельности	**Объект или область знания**	**Код и наименование профессиональной компетенции**	**Код и наименование индикатора достижения профессиональной компетенции**	**Основание (ПС, анализ иных требований, предъявляемых к выпускникам)**
Тип задач профессиональной деятельности: проектный				
Сбор и анализ детальной информации для формализации предметной области проекта и требований пользователей заказчика, интервьюирование ключевых сотрудников заказчика. Формирование и анализ требований к информатизации и автоматизации	Прикладные и информационные процессы Информационные системы Информационные технологии	ПК-1. Способность создавать и сопровождать требования и технические задания на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности	ПК-1.1. знает методы проведения обследования предприятия, сбора детальной информации о предприятии и ее структурирования ПК-1.2. умеет моделировать предметную область, используя современные формализмы, составлять технико-экономические обоснования	ПС 06.022 Системный аналитик

прикладных процессов, формализация предметной области проекта. Моделирование прикладных и информационных процессов. Составление технико-экономического обоснования проектных решений и технического задания на разработку информационной системы. Проектирование информационных систем по видам обеспечения. Программирование приложений, создание прототипа информационной системы			проектных решений и технические задания на разработку информационной системы ПК-1-3. владеет методами проектирования информационных систем по видам обеспечения, программирования приложений и создания прототипа информационной системы	
		ПК-3. Способность проводить анализ и выбор программно-технологических платформ, сервисов и информационных ресурсов информационной системы	ПК-3.1. знает основные современные программно-технологические платформы и их поставщиков, сервисы и информационные ресурсы информационной системы ПК-3.2. применять методы анализа и выбора программно-технологических платформ, сервисов и информационных ресурсов информационной системы ПК-3.3. владеет компьютерными средствами доступа к документации программно-технологических платформ, сервисам и информационным ресурсам информационных систем	Анализ иных требований проект ПООП 03.04.2019

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Тема 1. Введение в информационную безопасность (2 часа)

Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. Информационная безопасность как основа экономической безопасности предприятия.

Тема 2. Правовое обеспечение информационной безопасности (2 часа).

Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Права и обязанности работников предприятий по обеспечению информационной безопасности.

Тема 3. Организационное обеспечение информационной безопасности (2 часа).

Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия.

Тема 4. Современные угрозы сетевой безопасности (2 часа)

Основы сетевой безопасности. Способы нейтрализации сетевых атак, внедрение и практическое использование способов нейтрализации сетевых атак.

Тема 5. Технические средства и методы защиты информации (2 часа).

Инженерная защита объектов. Защита информации от утечки по техническим каналам. Методы и способы защиты информации на коммерческом предприятии.

Тема 6. Программно-аппаратные средства и методы обеспечения информационной безопасности (2 часа)

Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз.

Тема 7. Криптографические методы защиты информации (2 часа).

Симметричные и ассиметричные системы шифрования. Цифровые подписи (электронные подписи). Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ (последняя редакция). Инфраструктура открытых ключей. Криптографические протоколы.

Тема 8. Обеспечение безопасности сетевых устройств (2 часа)

Аутентификация конфигурирования открытого протокола кратчайшего пути (Open Shortest Path First, OSPF) с шифрованием Message Digest 5 (MD5) и Secure Hash Algorithm (SHA). Плоскости управления, менеджмента и данных с точки зрения использования ограничения плоскости управления (Control Plane Policing, CoPP).

Тема 9. Аутентификация, авторизация и учет (2 часа)

Основы Cisco Identify Services Engine (ISE). Управление устройствами и поддержание функций профилирования устройств, оценка состояния, управление гостевым доступом и доступ к сети на базе идентификации.

Тема 10. Внедрение технологий межсетевого экрана (2 часа)

Межсетевые экраны с фильтрацией пакетов, с сохранением состояния, шлюз прикладного уровня, прокси, с преобразованием адресов, на основе хостов, прозрачные и гибридные межсетевые экраны. Включение одного или нескольких межсетевых экранов в структуру защиты информации на предприятии.

Тема 11. Внедрение системы предотвращения вторжений (2 часа)

Реализация систем IDS или IPS. Типы доступных систем, локальные и сетевые подходы, способы размещения упомянутых систем, роли категорий сигнатур и возможные действия, которые сможет выполнять маршрутизатор Cisco IOS в случае обнаружения атаки.

Тема 12. Обеспечение безопасности локальной сети (LAN) (2 часа)

Обеспечение безопасности на границах сети производственного

предприятия. Защита оконечных устройств. Безопасность оконечных устройств. Защита устройств сетевой инфраструктуры локальной сети (LAN) и оконечных систем, к которым относятся рабочие станции, серверы, IP-телефоны, точки доступа и устройства сети хранения данных (SAN).

Тема 13. Внедрение виртуальных частных сетей (VPN) (2 часа)

Использование виртуальных частных сетей (VPN) в организациях для создания сквозного частного сетевого подключения через сторонние сети, через Интернет или экстранет. Протокол IP Security (IPsec). Безопасные сети VPN между двумя пунктами (site-to-site VPN).

Тема 14. Внедрение многофункционального устройства защиты Cisco Adaptive Security Appliance (2 часа)

Разновидности межсетевых экранов. Включение одного или нескольких межсетевых экранов, для обеспечения защиты ресурсов предприятия. Маршрутизатор ISR с функциями межсетевого экрана и многофункциональное устройство защиты (Adaptive Security Appliance, ASA). Основные сведения о платформе ASA.

Тема 15. Многофункциональное устройство обеспечения безопасности Cisco ASA с расширенным функционалом

Архитектура сетей без границ Cisco Secure Borderless Network. Серия устройств ASA 5500. Настройка конфигурации как в режиме командной строки, так и с помощью Менеджера устройств безопасности ASA (ASA Security Device Manager, ASDM). Начальные сведения об ASDM, а также о функциях межсетевого экрана и VPN, имеющихся на устройствах серии ASA 5505.

Тема 16. Управление безопасной сетью (2 часа)

Снижение риска сетевых атак на предприятии. Определение вероятных угроз и проведение анализа рисков. Планы и документы по обеспечению информационной безопасности и непрерывности работы в соответствии с изменениями потребностей организации.

Тема 17. Разработка комплексной политики безопасности (2 часа)

Цикл безопасной эксплуатации сети. Политика безопасности. Обзор политики безопасности. Структура политики безопасности. Технические политики и политики конечного пользователя. Стандарты, правила и процедуры политики безопасности.

Тема 18. Этические принципы работы в сфере кибербезопасности (2 часа)

Этические ценности специалиста по обеспечению кибербезопасности. Законы и ответственность, связанные с кибербезопасностью. Гражданское и уголовное законодательство и нормативные требования информационного и телекоммуникационного права. Отраслевые законы. Законы об уведомлении в случае нарушения безопасности. Защита конфиденциальности.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Лабораторная работа 1. Изучение методов шифрования с использованием методов активного обучения – работа в малых группах (2 часа)

Дешифрация предварительно зашифрованного сообщения с помощью шифра Vigenere. Создание сообщения, зашифрованного с помощью шифра Vigenere, и его дешифрация.

Лабораторная работа 2. Изучение сетевых атак и инструментов для аудита безопасности и проведения атак с использованием методов активного обучения – работа в малых группах (4 часа)

Изучение сетевых атак, организуемых злоумышленниками на сеть предприятия. Изучение инструментов аудита безопасности проведения атак.

Лабораторная работа № 3. Использование криптографических средств защиты информации коммерческого предприятия с использованием методов активного обучения – работа в малых группах (4 часа)

Создание зашифрованных файлов и криптоконтейнеров и их расшифрованние.

Лабораторная работа № 4. Реализация работы инфраструктуры открытых ключей с использованием методов активного обучения – работа в малых группах (4 часа)

Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи.

Лабораторная работа № 5. Средства стеганографии для защиты информации коммерческого предприятия с использованием методов активного обучения – работа в малых группах (4 часа)

Знакомство с средствами стеганографии. Использование средств стеганографии для защиты файлов.

Лабораторная работа № 6. Настройка безопасного сетевого соединения с использованием методов активного обучения – работа в малых группах (4 часа)

Создание защищенного канала связи между сотрудниками и отделами коммерческого предприятия средствами виртуальной частной сети.

Лабораторная работа № 7. Антивирусные средства защиты информации с использованием методов активного обучения – работа в малых группах (4 часа)

Изучение средств антивирусной защиты информации. Настройки средств антивирусной защиты информации. Типы вредоносного ПО.

Лабораторная работа 8. Защита маршрутизатора для административного доступа с использованием методов активного обучения – работа в малых группах: часть 1, часть 2 (2 часа)

Часть 1. Настройка основных параметров устройства. Подключение сетевых кабелей, как показано на топологической схеме. Настройка базовых параметров IP-адресации для маршрутизаторов компьютеров. Настройка OSPF-маршрутизации. Настройка хост-компьютеров. Проверка связи между хостами и маршрутизаторами.

Часть 2. Контроль административного доступа для маршрутизаторов. Настройка и шифрование всех паролей. Настройка предупреждающего баннера при входе в систему. Настройка расширенных функций безопасности. Настройка SSH-сервера на маршрутизаторе. Настройка SSH-клиента и проверка связи. Настройка SCP-сервера на маршрутизаторе

Лабораторная работа 9. Защита маршрутизатора для административного доступа с использованием методов активного обучения – работа в малых группах: часть 3, часть 4 (2 часа)

Часть 3. Настройка административных ролей. Создание нескольких представлений ролей и предоставление им различных привилегий. Проверка и сравнение представлений.

Часть 4. Настройка отчетов о защите и управлении Cisco IOS. Защита файлов образа и конфигурации Cisco IOS. Настройка функции SNMPv3 Security с помощью ACL. Настройка маршрутизатора в качестве источника синхронизированного времени для других устройств по протоколу NTP. Настройка поддержки Syslog на маршрутизаторе. Установка и активация сервера Syslog на компьютере. Внесение изменений на маршрутизаторе и отслеживание результатов в системном журнале на компьютере.

Лабораторная работа 10. Защита маршрутизатора для административного доступа с использованием методов активного обучения – работа в малых группах: часть 5, часть 6 (2 часа)

Часть 5. Защита плоскости управления. Настройка OSPF-аутентификации с помощью SHA256. Проверка OSPF-аутентификации

Часть 6. Настройка автоматизированных функций безопасности. Блокировка маршрутизатора с помощью Auto Secure и проверка конфигурации. Сравнение применения Auto Secure и защиты маршрутизатора вручную с помощью командной строки

Лабораторная работа 11. Защита административного доступа с помощью AAA и RADIUS с использованием методов активного обучения – работа в малых группах: часть 1, часть 2 (2 часа)

Часть 1. Настройка основных параметров.

Часть 2. Настройка локальной аутентификации.

Лабораторная работа 12. Защита административного доступа с помощью AAA и RADIUS с использованием методов активного обучения – работа в малых группах: часть 3 (2 часа)

Часть 3. Настройка локальной аутентификации с помощью AAA.

Лабораторная работа 13. Защита административного доступа с помощью AAA и RADIUS с использованием методов активного обучения – работа в малых группах: часть 4 (2 часа)

Часть 4. Настройка централизованной аутентификации с помощью AAA и RADIUS.

Лабораторная работа 14. Настройка зональных межсетевых экранов с использованием методов активного обучения – работа в малых группах (4 часа)

Часть 1. Основная конфигурация маршрутизаторов.

Часть 2. Настройка зонального межсетевого экрана (ZPF).

Лабораторная работа 15. Настройка системы предотвращения вторжений (IPS) с использованием методов активного обучения – работа в малых группах (4 часа)

Часть 1. Настройка базовых параметров маршрутизатора.

Часть 2. Настройка IOSIPS с помощью CLI.

Часть 3. Имитация атаки.

Лабораторная работа 16. Защита коммутаторов 2-го уровня с использованием методов активного обучения – работа в малых группах (4 часа)

Часть 1. Настройка базовых параметров коммутатора.

Часть 2. Настройка доступа к коммутаторам по SSH.

Часть 3. Настройка защищенных магистральных каналов и портов доступа.

Часть 4. Настройка IPDHCP Snooping.

Лабораторная работа 17. Настройка сети Site-to-Site VPN с помощью Cisco IOS с использованием методов активного обучения – работа в малых группах (4 часа)

Часть 1. Настройка основных параметров устройства.

Часть 2. Настройка сети Site-to-Site VPN с помощью Cisco IOS.

Лабораторная работа 18. Конфигурирование базовых настроек ASA и межсетевого экрана с использованием интерфейса командной строки (CLI): часть 1, часть 2 (2 часа)

Часть 1. Базовая настройка маршрутизатора/коммутатора/ПК.

Часть 2. Доступ к консоли ASA и конфигурирование базовых параметров с помощью режима настройки CLI.

Лабораторная работа 19. Конфигурирование базовых настроек ASA и межсетевого экрана с использованием интерфейса командной строки (CLI): часть 3, часть 4 (2 часа)

Часть 3. Настройка основных параметров ASA и уровней безопасности интерфейса с помощью интерфейса командной строки. Настройка имени хоста и доменного имени. Конфигурирование пароля для входа в систему и пароля привилегированного доступа. Установка даты и времени. Настройка внутреннего и внешнего интерфейсов. Проверка связи с ASA. Настройка доступа к ASA по SSH. Настройка на ASA доступа по HTTPS для ASDM.

Часть 4. Настройка маршрутизации, преобразования адресов и политики инспектирования с помощью интерфейса командной строки. Настройка статического маршрута по умолчанию для ASA. Настройка PAT и сетевых объектов. Изменение глобальной политики инспектирования приложений MPF.

Лабораторная работа 20. Конфигурирование базовых настроек ASA и межсетевого экрана с использованием интерфейса командной строки (CLI): часть 5, часть 6 (2 часа)

Часть 5. Настройка DHCP, AAA и SSH. Настройка ASA в качестве DHCP-сервера или клиента. Настройка локальной аутентификаци и пользователей AAA. Настройка удаленного доступа к ASA по SSH.

Часть 6. Настройка DMZ, статического преобразования NAT и ACL-списков. Настройка интерфейса DMZ VLAN 3 на ASA. Настройка статического преобразования NAT для сервера DMZ с помощью сетевого объекта. Настройка списка ACL, разрешающего доступ к серверу DMZ через

Интернет. Проверка доступа к серверу DMZ для внешних и внутренних пользователей.

Лабораторная работа 21. Конфигурирование сетей SSL VPN Any Connect для удаленного доступа с помощью ASDM: часть 1, часть 2 (2 часа)

Часть 1. Базовая настройка маршрутизатора/коммутатора/ПК. Подключение сетевых кабелей и сброс предыдущих настроек на устройствах, как показано на топологической схеме. Конфигурирование основных параметров для маршрутизаторов. Конфигурирование параметров IP для хостов. Проверка связи. Сохранение основной текущей конфигурации для каждого маршрутизатора и коммутатора.

Часть 2. Доступ к консоли ASA и ASDM. Доступ к консоли ASA. Сброс предыдущих настроек конфигурации ASA. Пропуск режима настройки. Настройка ASA с помощью скрипта CLI. Доступ к ASDM.

Лабораторная работа 22. Конфигурирование сетей SSL VPN Any Connect для удаленного доступа с помощью ASDM: часть 3 (2 часа)

Часть 3. Настройка сети SSL VPN с использованием клиента Any Connect с помощью ASDM. Запуск мастера VPN. Выбор протокола шифрования VPN. Выбор образа клиента, который нужно загрузить пользователям Any Connect. Настройка локальной аутентификации AAA. Настройка назначения клиентских адресов. Настройка разрешения сетевых имен Исключение преобразования адресов для VPN-трафика. Обзор варианта развертывания клиента Any Connect. Обзор экрана Summary и применение конфигурации для ASA.

Лабораторная работа 23. Конфигурирование сетей SSL VPN Any Connect для удаленного доступа с помощью ASDM: часть 4 (2 часа)

Часть 4. Подключение к AnyConnect SSL VPN. Проверка профиля клиента AnyConnect. Вход в систему с удаленного хоста. Обнаружение платформы (при необходимости). Автоматическая установка клиента Any

Connect VPN (при необходимости). Установка вручную клиента Any Connect VPN (при необходимости). Проверка связи по VPN.

Лабораторная работа 24. Комплексная лабораторная работа по курсу CCNA Security: часть 1, часть 2, часть 3 (2 часа)

Часть 1. Создание базовой технической политики безопасности.

Часть 2. Настройка основных параметров устройства.

Часть 3. Настройка защищенного административного доступа к маршрутизатору. Настройка зашифрованных паролей и баннера при входе в систему. Настройка времени ожидания для привилегированного режима на линиях консоли и VTY. Настройка частоты ошибок при входе в систему и расширений для входа в систему для VTY. Настройка доступа по протоколу Secure Shell (SSH) и отключение Telnet. Настройка локальной аутентификации пользователей по протоколу аутентификации, авторизации и учета (AAA). Защита маршрутизатора от атак методом подбора учетных данных, защита образа IOS и файла конфигурации. Настройка NTP-клиентов и NTP-сервера на маршрутизаторе. Настройка отчетности системного журнала маршрутизатора syslog и сервера syslog на локальном хосте.

Лабораторная работа 25. Комплексная лабораторная работа по курсу CCNA Security: часть 4, часть 5, часть 6 (2 часа)

Часть 4. Настройка зонального межсетевого экрана и системы предотвращения вторжений. Настройка зонального межсетевого экрана (ZPF) на ISR с помощью командной строки (CLI). Настройка системы предотвращения вторжений (IPS) на ISR с помощью командной строки (CLI)

Часть 5. Защита сетевых коммутаторов. Настройка паролей и баннера при входе в систему. Настройка доступа управляющей сети VLAN. Защита портов доступа. Защита от атак на Spanning Tree Protocol (STP). Настройка безопасности портов и отключение неиспользуемых портов.

Часть 6. Настройка основных параметров ASA и межсетевого экрана. Настройка основных параметров, паролей, даты и времени. Настройка внешних и внутренних интерфейсов VLAN. Настройка преобразования

адресов портов (PAT) для внутренней сети. Настройка сервера Dynamic Host Configuration Protocol (DHCP) для внутренней сети. Настройка административного доступа по протоколам Telnet и SSH. Настройка статического маршрута по умолчанию для многофункционального устройства безопасности (ASA). Настройка локальной аутентификации пользователей AAA. Настройка DMZ со статическим NAT и списком ACL. Проверка преобразования адресов и функций межсетевого экрана.

Лабораторная работа 26. Комплексная лабораторная работа по курсу CCNA Security: часть 7, часть 8, часть 9 (2 часа)

Часть 7. Настройка DMZ, статического NAT и списков контроля доступа (ACL) на ASA.

Часть 8. Настройка в ASA сети SSL VPN удаленного доступа без использования клиента с помощью ASDM. Настройка сети SSL VPN удаленного доступа с помощью диспетчера Adaptive Security Device Manager (ASDM). Проверка доступа к порталу посети SSL VPN.

Часть 9. Настройка сети Site-to-Site VPN между ASA и ISR. Настройка сети IPsec site-to-site VPN между ASA и маршрутизатором R3 с помощью ASDM и CLI. Активация и проверка туннеля IPsec site-to-site VPN между ASA и маршрутизатором R3.

САМОСТОЯТЕЛЬНАЯ РАБОТА

1. Теоретико-типологический анализ подборки периодической литературы по изучаемой дисциплин.

2. Составление глоссария терминов по изучаемой дисциплине.

3. Написание реферата.

4. Контрольное практическое задание (эссе).

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Информационная безопасность» включает в себя:

– план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

– характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

– требования к представлению и оформлению результатов самостоятельной работы;

– критерии оценки выполнения самостоятельной работы изложены в разделе VIII.

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	4 неделя	Теоретико-типологический анализ подборки периодической литературы по изучаемой дисциплине	9 часов	Устный опрос (УО-1)
2	8 неделя	Составление глоссария терминов по изучаемой дисциплине	9 часов	Устный опрос (УО-1)
3	12 неделя	Написание реферата	9 часов	Доклад (УО-3)
4	14 неделя	Контрольное практическое задание (эссе)	9 часов	Доклад (УО-3)
4	16 неделя	Подготовка к экзамену	36 час	Разно уровневые задачи (ПР-11)

Рекомендации по самостоятельной работе студентов

Самостоятельная работа студентов состоит из подготовки к практическим занятиям, работы над рекомендованной литературой,

написания докладов по теме семинарского занятия, подготовки презентаций, решения задач.

При организации самостоятельной работы преподаватель должен учитывать уровень подготовки каждого студента и предвидеть трудности, которые могут возникнуть при выполнении самостоятельной работы. Преподаватель дает каждому студенту индивидуальные и дифференцированные задания. Некоторые из них могут осуществляться в группе (например, подготовка доклада и презентации по одной теме могут делать несколько студентов с разделением своих обязанностей – один готовит научно-теоретическую часть, а второй проводит анализ практики).

Методические указания к проведению теоретико-типологического анализа подборки периодической литературы по изучаемой дисциплине

Сообщения должны включать в себя библиографические списки литературы и рефераты по всем темам изучаемой дисциплины.

Список литературы должен содержать не менее 30 источников, они должны быть перечислены в алфавитном порядке, соблюдена нумерация. Список литературы должен быть оформлен по принципу реферативной работы, в обязательном порядке присутствует титульный лист и нумерация страниц. Объем работы должен составлять 10-15 страниц.

Оформление электронных ресурсов в списке литературы при ссылке на авторов выполняется согласно п.п. 4.14.1 Оформление списка литературы Процедуры ВКР ДВФУ (см. пример в Процедуре).

Оформление электронных ресурсов в списке литературы при ссылке на сайты и порталы (если не указаны авторы) рекомендуется оформлять отдельным перечнем интернет-ресурсов в общей нумерации списка литературы (в конце списка) согласно следующему примеру:

Интернет-ресурсы:

Расчёт совокупной стоимости владения (TCO). URL: http://www.akvalis.ru/service/67/. Дата обращения: 28.05.2014 г.

Тема 2. Составление глоссария терминов по изучаемой дисциплине.

Методические указания к составлению глоссария

Глоссарий охватывает все узкоспециализированные термины, встречающиеся в тексте. Глоссарий должен содержать не менее 50 терминов, они должны быть перечислены в алфавитном порядке, соблюдена нумерация. Глоссарий должен быть оформлен по принципу реферативной работы, в обязательном порядке присутствует титульный лист и нумерация страниц. Объем работы должен составлять 5-10 страниц. Тщательно проработанный глоссарий помогает избежать разночтений и улучшить в целом качество всей документации. В глоссарии включаются самые частотные термины и фразы, а также все ключевые термины с толкованием их смысла. Глоссарии могут содержать отдельные слова, фразы, аббревиатуры, слоганы и даже целые предложения.

Тема 3. Написание реферата по теме, предложенной преподавателем или самостоятельно выбранной студентом и согласованной с преподавателем.

Методические указанию к выполнению реферата

Цели и задачи реферата

Реферат (от лат. refero — докладываю, сообщаю) представляет собой краткое изложение проблемы практического или теоретического характера с формулировкой определенных выводов по рассматриваемой теме. Избранная студентом проблема изучается и анализируется на основе одного или нескольких источников. В отличие от курсовой работы, представляющей собой комплексное исследование проблемы, реферат направлен на анализ одной или нескольких научных работ.

Целями написания реферата являются:

- развитие у студентов навыков поиска актуальных проблем современного законодательства;

- развитие навыков краткого изложения материала с выделением лишь самых существенных моментов, необходимых для раскрытия сути проблемы;

- развитие навыков анализа изученного материала и формулирования собственных выводов по выбранному вопросу в письменной форме, научным, грамотным языком.

Задачами написания реферата являются*:*

- научить студента максимально верно передать мнения авторов, на основе работ которых студент пишет свой реферат;

- научить студента грамотно излагать свою позицию по анализируемой в реферате проблеме;

- подготовить студента к дальнейшему участию в научно – практических конференциях, семинарах и конкурсах;

- помочь студенту определиться с интересующей его темой, дальнейшее раскрытие которой возможно осуществить при написании курсовой работы или диплома;

- уяснить для себя и изложить причины своего согласия (несогласия) с мнением того или иного автора по данной проблеме.

Основные требования к содержанию реферата

Студент должен использовать только те материалы (научные статьи, монографии, пособия), которые имеют прямое отношение к избранной им теме. Не допускаются отстраненные рассуждения, не связанные с анализируемой проблемой. Содержание реферата должно быть конкретным, исследоваться должна только одна проблема (допускается несколько, только если они взаимосвязаны). Студенту необходимо строго придерживаться логики изложения (начать с определения и анализа понятий, перейти к постановке проблемы, проанализировать пути ее решения и сделать соответствующие выводы). Реферат должен заканчиваться выведением выводов по теме.

По своей структуре реферат состоит из:

1.Титульного листа;

2.Введения, где студент формулирует проблему, подлежащую анализу и исследованию;

3.Основного текста, в котором последовательно раскрывается избранная тема. В отличие от курсовой работы, основной текст реферата предполагает разделение на 2-3 параграфа без выделения глав. При необходимости текст реферата может дополняться иллюстрациями, таблицами, графиками, но ими не следует "перегружать" текст;

4. Заключения, где студент формулирует выводы, сделанные на основе основного текста.

5.Списка использованной литературы. В данном списке называются как те источники, на которые ссылается студент при подготовке реферата, так и иные, которые были изучены им при подготовке реферата.

Объем реферата составляет 10-15 страниц машинописного текста, но в любом случае не должен превышать 15 страниц. Интервал – 1,5, размер шрифта – 14, поля: левое — 3см, правое — 1,5 см, верхнее и нижнее — 1,5 см.. Страницы должны быть пронумерованы. Абзацный отступ от начала строки равен 1,25 см.

Порядок сдачи реферата и его оценка

Реферат пишется студентами в течение триместра в сроки, устанавливаемые преподавателем по конкретной дисциплине, и сдается преподавателю, ведущему дисциплину.

По результатам проверки студенту выставляется определенное количество баллов, которое входит в общее количество баллов студента, набранных им в течение триместра. При оценке реферата учитываются соответствие содержания выбранной теме, четкость структуры работы, умение работать с научной литературой, умение ставить проблему и анализировать ее, умение логически мыслить, владение профессиональной терминологией, грамотность оформления.

Контрольное практическое задание (эссе)

Обучающимся предлагается написать эссе по теме: «Что такое «Информационная безопасность».

Рекомендации по структуре и содержанию эссе:

1. Приведите формулировку информационной безопасности;

2. Опишите основные подходы к этому понятию;

3. Укажите основные проблемы, связанные с определением этого понятия.

4. В заключение сделайте выводы о современном состоянии данного вопроса.

Методические рекомендации по подготовке эссе

Эссе – вид самостоятельной исследовательской работы студентов, с целью углубления и закрепления теоретических знаний и освоения практических навыков. Цель эссе состоит в развитии самостоятельного творческого мышления и письменного изложения собственных мыслей.

В зависимости от темы формы эссе (его части) могут быть различными. Это может быть анализ имеющихся статистических данных по изучаемой проблеме, анализ материалов из СМИ и подробный разбор проблемной ситуации с развернутыми мнениями, подбором и детальным анализом примеров, иллюстрирующих проблему и т.п.

В процессе выполнения эссе, обучающемуся предстоит выполнить следующие виды работ: составить план эссе; отобрать источники, собрать и проанализировать информацию по проблеме; систематизировать и проанализировать собранную информацию; представить проведенный анализ с собственными выводами и предложениями.

Эссе выполняется студентом самостоятельно. При возникновении у студента вопросов, он может обратиться к преподавателю.

Введение – состоит из ряда компонентов, связанных логически и стилистически. Во введении рекомендуется отразить материал по первым двум пунктам структуры эссе. При работе над введением могут возникнуть

вопросы: надо ли давать определения терминам? Почему тема является актуальной в настоящий момент?

Текстовое изложение материала (основная часть) – теоретико-практическое изложение основных пунктов по структуре эссе. Данная часть предполагает развитие аргументации и анализа, а также обоснование их, исходя из имеющихся данных, других аргументов и позиций по этому вопросу. Большое значение имеют подзаголовки, на основе которых осуществляется аргументация; именно здесь необходимо обосновать предлагаемую аргументацию/анализ. В качестве аналитического инструмента можно использовать графики, диаграммы, схемы (рисунки) так, где это необходимо. Традиционно в научном познании анализ может проводиться с использованием следующих категорий: причина-следствие, общее-особенное, форма-содержание, часть-целое, постоянство-изменчивость. В пределах параграфа необходимо ограничить себя рассмотрением одной главной мысли.

Таким образом, основная часть – рассуждение и аргументация. В этой части необходимо представить релевантные теме концепции, суждения и точки зрения, привести основные аргументы «за» и «против» них, сформулировать свою позицию и аргументировать ее.

Заключение – обобщения и аргументированные выводы по теме эссе с указанием области ее применения. Оно подытоживает эссе или еще раз вносит пояснения изложенного в основной части и предложения автора. В заключительной части эссе должны быть сформулированы выводы и определено их приложение к практической области деятельности.

Список литературы составляет одну из частей работы, отражающей самостоятельную творческую работу автора и позволяющей судить о степени фундаментальности данной работы. При составлении списка в перечень включаются только те источники, которые действительно были использованы при подготовке эссе.

При написании эссе необходимо понять сущность фактического материала, связанного с темой, и продемонстрировать это в эссе.

Требования к оформлению эссе. Поскольку эссе является письменной работой, обучающимся рекомендуется при оформлении соблюдать требования, предъявляемые к оформлению письменных работ студентов ДВФУ: шрифт Times New Roman, кегль 14, интервал 1,5, выравнивание по ширине, параметры страниц: слева - 3, справа – 1,5, вверху и внизу – по 2 см, нумерация страниц – внизу справа. Объем эссе не более 5 страниц.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Темы 1, 2, 3, 4, 5, 6, 7, 8	ПК-1	знает методы проведения обследования предприятия, сбора детальной информации о предприятии и ее структурирования	Самостоятельная работа 1, 2. Собеседование (УО-1)	Вопросы к экзамену 1-30
			умеет моделировать предметную область, используя современные формализмы, составлять технико-экономические обоснования проектных решений и технические задания на разработку информационной системы		
			владеет методами проектирования информационных систем по видам обеспечения, программирования приложений и создания прототипа информационной системы		
2	Темы 9, 10, 11, 12, 13, 14, 15, 16	ПК-1	знает методы проведения обследования предприятия, сбора детальной информации о предприятии и ее структурирования	Самостоятельная работа 3,4. Собеседование (УО-1)	Вопросы к экзамену 31 60
			умеет моделировать предметную область, используя современные формализмы, составлять технико-экономические обоснования проектных решений и технические задания на разработку информационной		

			системы		
			владеет методами проектирования информационных систем по видам обеспечения, программирования приложений и создания прототипа информационной системы		
3	Темы 1-16	ПК-3	знает основные современные программно-технологические платформы и их поставщиков, сервисы и информационные ресурсы информационной системы	Тест «Итоговый тест» (УО-3)	Вопросы к экзамену 1-30
			Уметь применять методы анализа и выбора программно-технологических платформ, сервисов и информационных ресурсов информационной системы		
			владеет компьютерными средствами доступа к документации программно-технологических платформ, сервисам и информационным ресурсам информационных систем		

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в соответствующих разделах программы.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Лелюхин С. Е. Экономическая безопасность в предпринимательской деятельности : учебник / С. Е. Лелюхин, А. М. Коротченков, У. В. Данилова : Москва : Проспект, 2016. 20 экземпляров.

2. Шаханова М. В. Современные технологии информационной безопасности : учебнометодический комплекс / Шаханова ; Дальневосточный федеральный университет : Москва : Проспект, 2015. 7 экземпляров.

3. Платонов В. В. Программно-аппаратные средства защиты информации : учебник для вузов / В. В. Платонов. 2-е изд., стер. Москва : Академия, 2014. 15 экземпляров.

Дополнительная литература

1. Фомин, Д. В. Информационная безопасность : учебно-методическое пособие для студентов заочной формы обучения направления подготовки 38.03.05 «Бизнес-информатика» / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 125 c. — ISBN 978-5-4487-0299-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/77318.html (дата обращения: 05.10.2019).

2. Горюхина, Е. Ю. Информационная безопасность : учебное пособие / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева. — Воронеж : Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. — 221 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72672.html (дата обращения: 05.10.2019).

3. Партыка Т. Л., Попов И. И. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. 5-е изд., перераб. и доп. М.: Форум: НИЦ ИНФРА-М, 2014. 432 с.: ил.; 60x90 1/16. (Профессиональное образование). (переплет) ISBN 978-5-91134-627-0 Режим доступа: http://znanium.com/catalog/product/420047

Ресурсы сети Интернет

1. Электронный курс Сетевой Академии Cisco «Введение в кипербезопасность» [электронный ресурс]. Режим доступа: https://static-course-assets.s3.amazonaws.com/CyberSec2/ru/index.html#0.0.1.1

2. Электронный курс Сетевой Академии Cisco «Cybersecurity Essentials» [электронный ресурс]. Режим доступа: https://static-course-assets.s3.amazonaws.com/CyberEss/ru/index.html#0.0

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Рекомендации по планированию и организации времени, отведенного на изучение дисциплины

Рекомендуется планировать и организовать время, отведенное на изучение дисциплины, следующим образом:

– изучение теоретического материала по источникам литературы – 2 часа в неделю;

– подготовка к практическому занятию – 1 час;

– выполнение практического задания – 1 час.

Всего в неделю в среднем – 4 часа.

Описание последовательности действий обучающихся, или алгоритм изучения дисциплины

При изучении дисциплины очень полезно самостоятельно изучать материал. Тогда лекция будет гораздо понятнее. Для понимания материала и качественного его усвоения рекомендуется такая последовательность действий:

1. В течение недели выбрать время (2 часа) для работы с рекомендованной литературой в библиотеке или ресурсами Интернет.

2. При подготовке к практическим занятиям следующего дня, необходимо сначала повторить пройденный теоретический материал предыдущего занятия по теме домашнего задания. При выполнении упражнения нужно сначала понять, что требуется, какой теоретический материал нужно использовать.

Рекомендации по использованию LMS Blackboard

При освоении дисциплины «Информационная безопасность» необходимо ознакомиться с приказами ректора ДВФУ: ПРИКАЗ № 12-13-73 от 23.01.2015 «Об утверждении Регламента Экспертизы выпускных квалификационных работ _студентов на н (1382763 v1)» и ПРИКАЗ № 12-13-382 от 25.04.2013 «Об обеспечении самостоятельности выполнения

письменных работ обучающимися ДВФУ с использованием модуля «SafeAssign» интегрированной платформы электронного обучения LMS (Blackboard)».

В соответствии с этими документами на плагиат могут проверяться не только ВКР, но и другие учебные работы. В этих документах преподавателю дано право самостоятельно оценивать уровень уникальности учебных работ. При проверке учебных работ также оценивается их оформление согласно Процедуры ВКР ДВФУ.

Для входа в LMS Blackboard Collaborate (BBC) необходимо установить модуль запуска Blackboard Collaborate Launcher, а затем при загрузке BBC необходимо переименовать файл meeting.collab в meeting.jnlp (переименовать расширение этого файла). Это можно сделать следующим образом: при загрузке файла meeting.collab выбрать опцию «Сохранить как» и через точку без пробелов дописать к нему расширение jnlp. Файл можно сохранить на Рабочий стол и затем запустить его, дважды щёлкнув по нему мышкой. Остальные действия – согласно сообщениям, в появляющихся окнах. Это необходимо делать каждый раз при запуске сессии.

Ниже, на рисунках 1, 2, 3, 4, прилагаются скриншоты с предлагаемыми действиями для запуска BBC. Предлагаемые действия также описаны в LMS Blackboard по ссылке Мой кабинет и в окне при загрузке BBC.

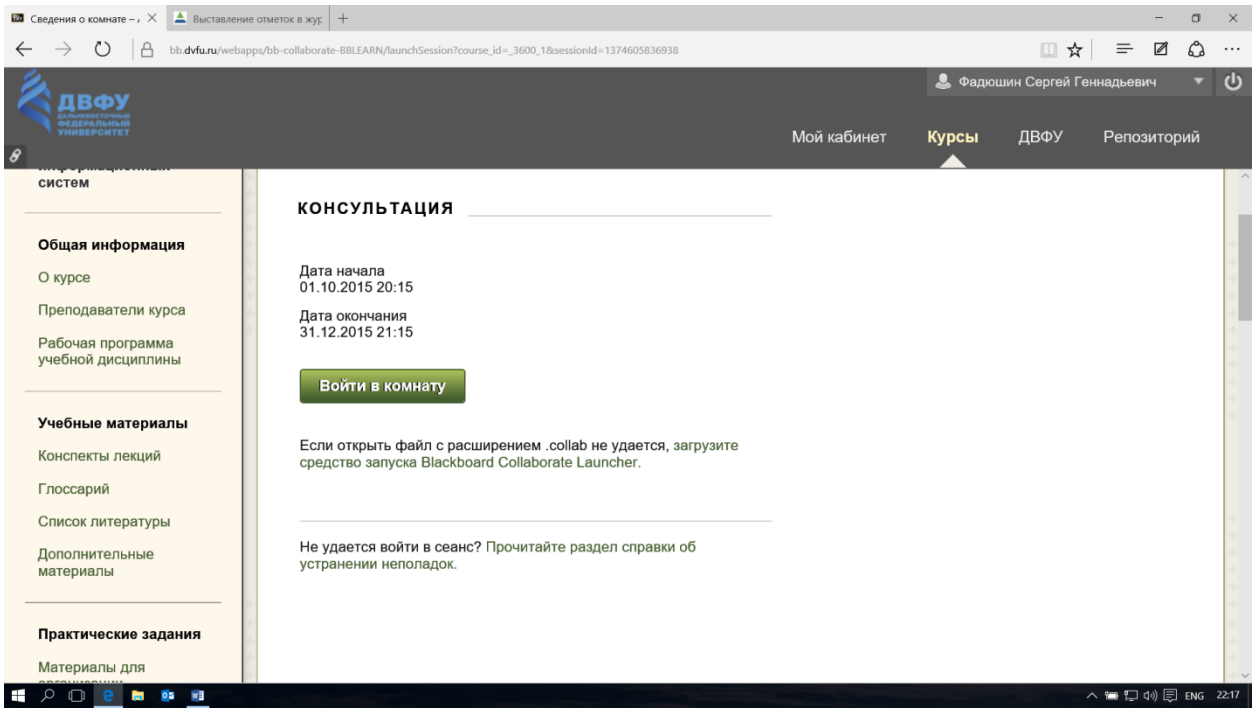

Рисунок 1

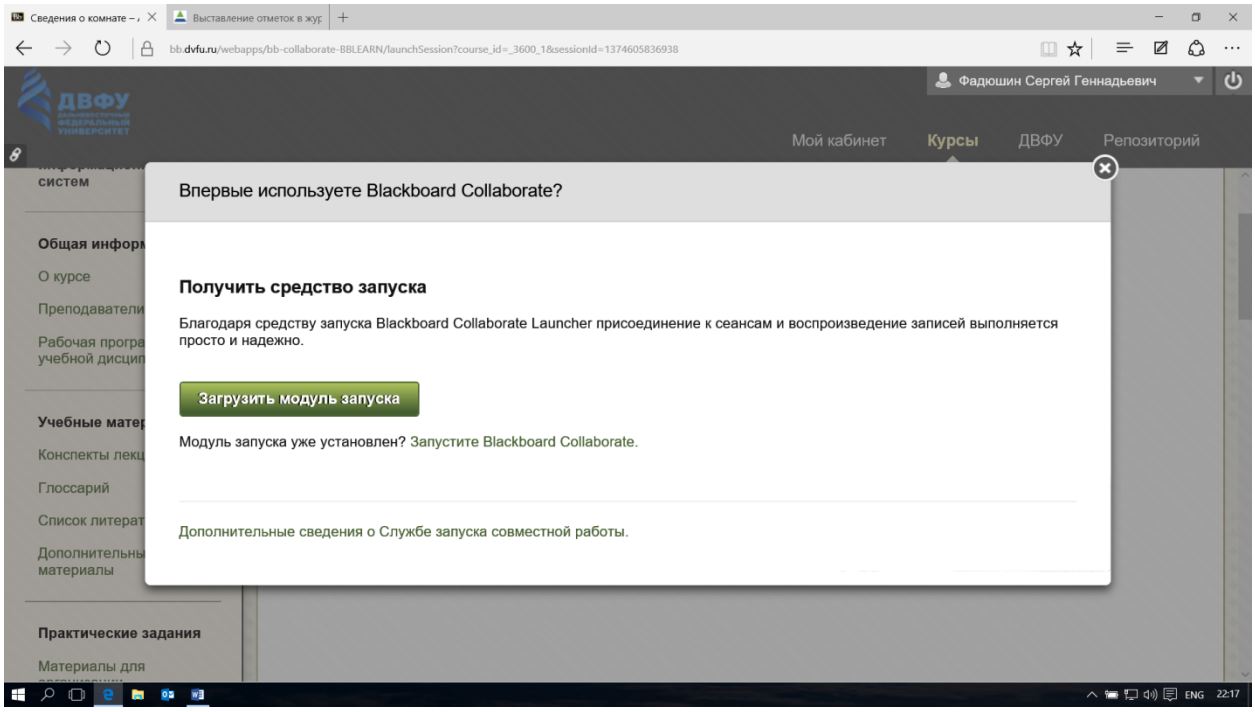

Рисунок 2

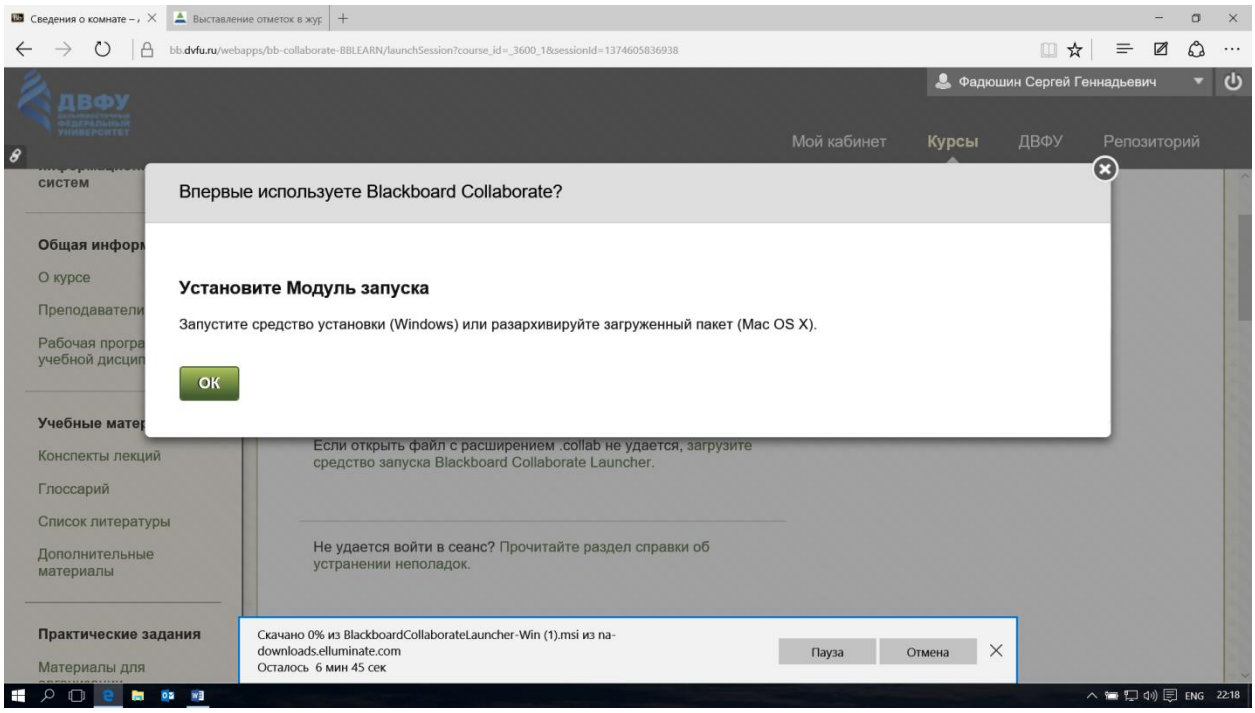

Рисунок 3

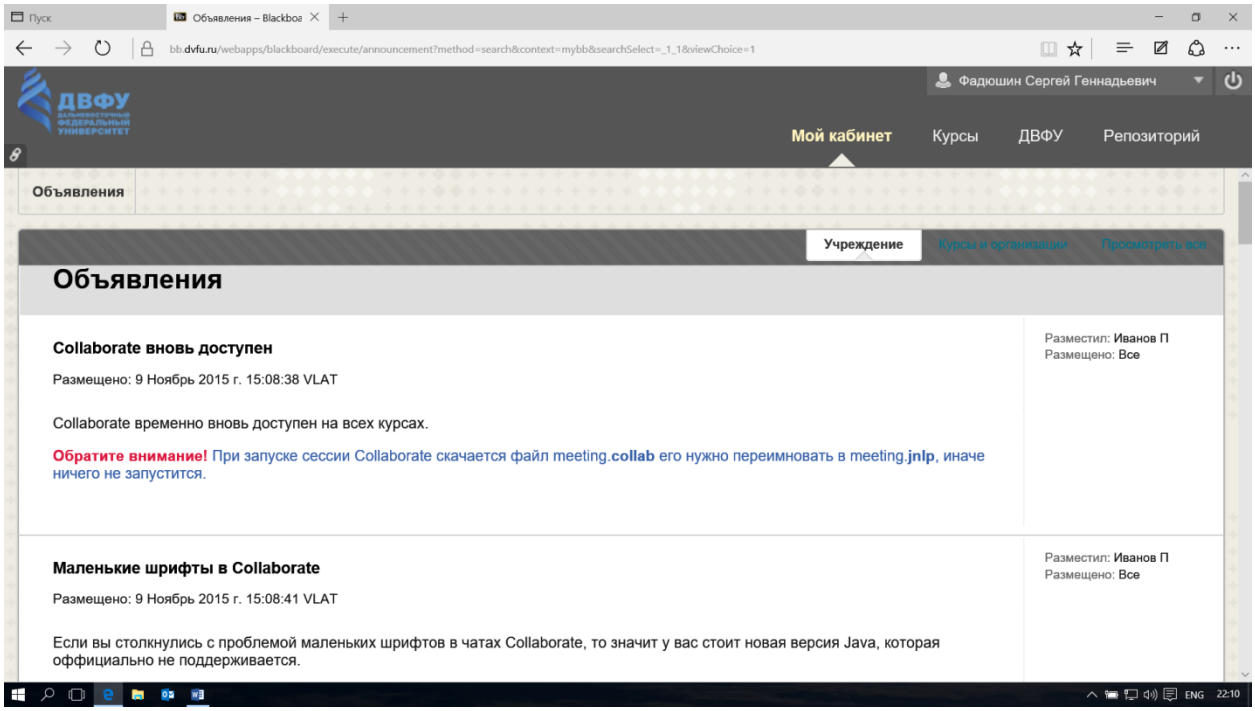

Рисунок 4

При сдаче экзамена в режиме on-line зайдите в LMS Blackboard по адресу bb.dvfu.ru, который вводится в адресной строке браузера (браузер может быть любой, кроме Opera) на электронный учебный курс «Информационная безопасность». Выберите ссылку «Экзамен». В окне справа будут указаны вопросы и порядок сдачи экзамена. Как будете готовы – сообщите. Для сдачи экзамена необходимо зайти в LMS Blackboard Collaborate по ссылке «Виртуальная аудитория». Справа в окне нажать на ссылку «Информационная безопасность», а затем положительно ответить на все вопросы, которые будут появляться в окнах. Заблаговременно настройте LMS Blackboard Collaborate, т.к. потребуется установка ПО Java и настройка безопасности.

Рекомендации по работе с литературой

Основным методом самостоятельного овладения знаниями является работа с литературой. Это сложный процесс, требующий выработки определенных навыков, поэтому студенту нужно обязательно научиться работать с книгой.

Осмысление литературы требует системного подхода к освоению материала. В работе с литературой системный подход предусматривает не только внимательное чтение текста и изучение специальной литературы, но и обращение к дополнительным источникам – справочникам, энциклопедиям, словарям, которые являются основными помощниками в самостоятельной работе студента, так как глубокое изучение именно их материалов позволит студенту освоить новую научную терминологию, а затем самостоятельно оперировать теоретическими категориями и понятиями. Такого рода работа с литературой обеспечивает решение студентом поставленной перед ним задачи (подготовка к семинарскому занятию, выполнение практических заданий и т.д.).

Литература для изучения обычно выбирается из списка литературы, выданного преподавателем, либо путем самостоятельного отбора

материалов. После этого непосредственно начинается изучение материала, изложенного в источнике.

При изучении материала источника необходимо обращать особое внимание на комментарии и примечания, которыми сопровождается текст. Они разъясняют отдельные места текста, дополняют изложенный материал, указывают ссылки на цитируемые источники, исторические сведения о лицах, фактах, объясняют малоизвестные или иностранные слова.

Во время изучения литературы следует конспектировать и составлять рабочие записи прочитанного, которые могут быть сделаны и в виде простого и развернутого плана, цитирования, тезисов, резюме, аннотации, конспекта. Такие записи удлиняют процесс проработки, изучения книги, но способствуют ее лучшему осмыслению и усвоению, выработке навыков кратко и точно излагать материал.

Наиболее надежный способ собрать нужный материал составить конспект краткое изложение своими словами содержания книги. Конспекты позволяют восстановить в памяти ранее прочитанное без дополнительного обращения к самой книге. При их составлении следует пользоваться различными приемами выделения отдельных частей текста, ключевых выражений, терминов, основных понятий (выделение абзацев, подчеркивание, написание жирным шрифтом, курсивом, использование цветных чернил и т.п.). Желательно оставлять поля для внесения дополнений, поправок или фиксации собственных мыслей по данной записи, возможно несовпадающих с авторской точкой зрения.

При изучении литературы особое внимание следует обращать на новые термины и понятия. Понимание сущности и значения терминов способствует формированию способности логического мышления, приучает мыслить абстракциями, что важно при усвоении дисциплины. Поэтому при изучении темы курса студенту следует активно использовать универсальные и специализированные энциклопедии, словари, иную справочную литературу.

Вся рекомендуемая для изучения курса литература подразделяется на основную и дополнительную. К основной литературе относятся источники, необходимые для полного и твердого усвоения учебного материала. Необходимость изучения дополнительной литературы диктуется, прежде всего тем, что в учебной литературе нередко остаются неосвещенными современные проблемы, а также не находят отражение новые документы, события, явления, научные открытия последних лет. Поэтому дополнительная литература рекомендуется для более углубленного изучения программного материала.

Рекомендации по подготовке к экзамену

Экзамен это заключительный этап изучения дисциплины, имеющий целью проверить теоретические знания студента, его навыки и умение применять полученные знания при решении практических задач. Экзамен проводится в объеме учебной программы по дисциплине в устной форме.

Подготовка к экзамену начинается с первого занятия по дисциплине, на котором студенты получают общую установку преподавателя и перечень основных требований к текущей и промежуточной аттестации. При этом важно с самого начала планомерно осваивать материал, руководствуясь, прежде всего, перечнем вопросов, конспектировать важные для решения учебных задач источники. В течение семестра происходят пополнение, систематизация и корректировка студенческих наработок, освоение нового и закрепление уже изученного материала.

Дисциплина «Информационная безопасность» разбита на темы, которые представляют собой логически завершенные части рабочей программы курса и являются тем комплексом знаний и умений, которые подлежат контролю.

Практические задания являются важными этапами подготовки к экзамену, поскольку позволяют студенту оценить уровень собственных знаний и своевременно восполнить имеющиеся пробелы.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для обеспечения учебного процесса по дисциплине «Информационная безопасность» используется следующее материально-техническое обеспечение: компьютеры, операционная система Windows, Интернет, текстовый редактор MS Word, табличный процессор MS Excel, компьютерный класс, LMS Blackboard, LMS Blackboard Collaborate, персональные компьютеры студентов.

VIII. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Паспорт ФОС

Задача профессиональной деятельности	Объект или область знания	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции	Основание (ПС, анализ иных требований, предъявляемых к выпускникам)
Тип задач профессиональной деятельности: проектный				
Сбор и анализ детальной информации для формализации предметной области проекта и требований пользователей заказчика, интервьюирование ключевых сотрудников заказчика. Формирование и анализ требований к информатизации и автоматизации прикладных процессов, формализация предметной области проекта. Моделирование прикладных и информационных процессов. Составление технико-экономического обоснования проектных решений и технического задания на разработку информационной системы. Проектирование	Прикладные и информационные процессы Информационные системы Информационные технологии	ПК-1. Способность создавать и сопровождать требования и технические задания на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности	ПК-1.1. знает методы проведения обследования предприятия, сбора детальной информации о предприятии и ее структурирования ПК-1.2. умеет моделировать предметную область, используя современные формализмы, составлять технико-экономические обоснования проектных решений и технические задания на разработку информационной системы ПК-1-3. владеет методами проектирования информационных систем по видам обеспечения, программирования приложений и создания прототипа информационной системы	ПС 06.022 Системный аналитик
		ПК-3.	ПК-3.1.	Анализ иных

информационных систем по видам обеспечения. Программирование приложений, создание прототипа информационной системы		Способность проводить анализ и выбор программно-технологических платформ, сервисов и информационных ресурсов информационной системы	знает основные современные программно-технологические платформы и их поставщиков, сервисы и информационные ресурсы информационной системы ПК-3.2. применять методы анализа и выбора программно-технологических платформ, сервисов и информационных ресурсов информационной системы ПК-3.3. владеет компьютерными средствами доступа к документации программно-технологических платформ, сервисам и информационным ресурсам информационных систем	требований проект ПООП 03.04.2019

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Темы 1, 2, 3, 4, 5, 6, 7, 8	ПК-1	знает методы проведения обследования предприятия, сбора детальной информации о предприятии и ее структурирования	Самостоятельная работа 1. Изучение электронного курса Сетевой Академии Cisco	Вопросы к экзамену 1 15

			умеет моделировать предметную область, используя современные формализмы, составлять технико-экономические обоснования проектных решений и технические задания на разработку информационной системы	«Введение в кипербезопасность», собеседование (УО-1)	
			владеет методами проектирования информационных систем по видам обеспечения, программирования приложений и создания прототипа информационной системы		
2	Темы 9, 10, 11, 12, 13, 14, 15, 16	ПК-1	знает методы проведения обследования предприятия, сбора детальной информации о предприятии и ее структурирования	Самостоятельная работа 2. Изучение электронного курса Сетевой Академии Cisco «Cybersecurity Essentials», собеседование (УО-1)	Вопросы к экзамену 16 30
			умеет моделировать предметную область, используя современные формализмы, составлять технико-экономические обоснования проектных решений и технические задания на разработку информационной системы		
			владеет методами проектирования информационных систем по видам обеспечения, программирования приложений и создания прототипа информационной системы		
3	Темы 1-16	ПК-3	знает основные современные программно-	Тест «Итоговый тест» (УО-3)	Вопросы к экзамену 1-30

			технологические платформы и их поставщиков, сервисы и информационные ресурсы информационной системы		
			Уметь применять методы анализа и выбора программно-технологических платформ, сервисов и информационных ресурсов информационной системы		
			владеет компьютерными средствами доступа к документации программно-технологических платформ, сервисам и информационным ресурсам информационных систем		

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
ПК-1. Способность создавать и сопровождать требования и технические задания на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности	знает (пороговый уровень)	Основные понятия создания и сопровождения требований и технических заданий на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности	Знание основных понятий создания и сопровождения требований и технических заданий на разработку, и модернизацию систем и подсистем малого и среднего масштаба, и сложности; знание основных понятий по информатике и информационным технологиям;	Способность дать определения основных понятий создания и сопровождения требований и технических заданий на разработку, и модернизацию систем и подсистем малого и среднего масштаба, и сложности; способность перечислить и раскрыть суть основных понятий создания и сопровождения требований и технических заданий на

				разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности
	умеет (продвинутый)	Документировать процессы создания и сопровождения требований и технических заданий на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности	Умение работать с техническими заданиями на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности	способность работать с техническими заданиями на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности
	владеет (высокий)	Методами создания технических заданий на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности	Владение методами создания технических заданий на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности	способность бегло и точно применять терминологический аппарат по методам создания технических заданий на разработку, и модернизацию систем и подсистем малого и среднего масштаба и сложности
ПК-3. Способность проводить анализ и выбор программно-технологических платформ, сервисов и информационных ресурсов информационной системы	знает (пороговый уровень)	Основные понятия анализа и выбора программно-технологических платформ, сервисов и информационных ресурсов информационной системы	Знание основных понятий анализа и выбора программно-технологических платформ, сервисов и информационных ресурсов информационной системы	Способность дать определения основных понятий по анализу и выбору программно-технологических платформ, сервисов и информационных ресурсов информационной системы
	умеет (продвинутый)	Осуществлять анализ и выбор программно-технологических платформ, сервисов и информационных ресурсов информационной системы	Умение осуществлять анализ и выбор программно-технологических платформ, сервисов и информационных ресурсов информационной системы	способность осуществлять анализ и выбор программно-технологических платформ, сервисов и информационных ресурсов информационной системы
	владеет (высокий)	Методами анализа и выбора программно-технологических платформ, сервисов и информационных ресурсов информационной системы	Владение методами анализа и выбора программно-технологических платформ, сервисов и информационных ресурсов информационной системы	способность бегло и точно применять терминологический аппарат анализа и выбора программно-технологических платформ, сервисов и информационных ресурсов информационной системы

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Текущая аттестация студентов. Текущая аттестация студентов по дисциплине «Информационная безопасность» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация по дисциплине «Информационная безопасность» проводится в форме контрольных мероприятий (работа на семинарских занятиях, выполнение практических заданий, доклад, сообщение) по оцениванию фактических результатов обучения студентов и осуществляется ведущим преподавателем.

Объектами оценивания выступают:

– учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

– степень усвоения теоретических знаний;

– уровень овладения практическими умениями и навыками по всем видам учебной работы;

– результаты самостоятельной работы.

Краткая характеристика оценочных средств:

– УО-1 Собеседование средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

– УО-3 Доклад, сообщение продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы

– УО-4 Круглый стол, дискуссия, полемика, диспут, дебаты

оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения.

– ПР-1 – Тест – система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающихся.

– ПР-11 Разноуровневые задачи реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей; творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.

Критерии оценки устных ответов

- 100-85 баллов если ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.
- 85-76 баллов ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна две неточности в ответе.

- 75-61 балл – оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.
- 60-50 баллов – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценки письменных ответов

- 100-86 баллов если ответ показывает глубокое и систематическое знание всего программного материала и структуры конкретного вопроса, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Знание основной литературы и знакомство с дополнительно рекомендованной литературой. Логически корректное и убедительное изложение ответа.
- 85-76 баллов знание узловых проблем программы и основного содержания лекционного курса; умение пользоваться концептуально-понятийным аппаратом в процессе анализа основных проблем в рамках данной темы; знание важнейших работ из списка рекомендованной

литературы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа.

- 75-61 балл – фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ.
- 60-50 баллов – незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе.

Примерные темы докладов, сообщений

1. Основные угрозы информационной безопасности.
2. Модели информационной безопасности.
3. Методы защиты информации.
4. Правовые методы защиты информации.
5. Организационные методы защиты информации.
6. Технические методы защиты информации.
7. Программно-аппаратные методы защиты информации.
8. Криптографические методы защиты информации.
9. Физические методы защиты информации.
10. Главные государственные органы в области обеспечения информационной безопасности.
11. Виды защищаемой информации.
12. Основные законы в области защиты информации в РФ.
13. Основные цели и задачи РФ в области обеспечения информационной безопасности
14. Концепция информационной безопасности.

15. Доктрина информационной безопасности Российской Федерации.

16. Профессиональная тайна.

17. Основные международные стандарты в области информационной безопасности.

18. Стандарт ГОСТ Р ИСО/МЭК 27002-2014.

19. Политика безопасности.

20. Технические каналы утечки информации.

21. Виды компьютерных угроз.

22. Средства стенографической защиты информации.

23. Симметричные алгоритмы шифрования.

24. Ассиметричные алгоритмы шифрования.

25. Криптографическая хеш-функция.

26. Цифровая подпись.

27. Инфраструктура открытых ключей.

28. Российские и международные стандарты на формирование цифровой подписи.

29. Основные криптографические протоколы, используемые в сетях.

30. Современные технологии информационной безопасности.

Контрольное практическое задание (эссе)

Обучающимся предлагается написать эссе по теме: «Что такое информационная безопасность».

Рекомендации по структуре и содержанию эссе:

1. Приведите формулировку информационной безопасности;

2. Опишите основные подходы к этому понятию;

3. Укажите основные проблемы, связанные с определением этого понятия.

4. В заключение сделайте выводы о современном состоянии данного вопроса.

Критерии оценки (письменных заданий, доклада, эссе, в том числе выполненных в форме презентаций)

- 100-86 баллов выставляется студенту, если студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент знает и владеет навыком самостоятельной исследовательской работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно
- 85-76 баллов работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы
- 75-61 балл – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы
- 60-50 баллов если работа представляет собой пересказанный или полностью переписанный исходный текст без каких-либо комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценки презентации доклада:

Оценка	50-60 баллов (неудовлетворительно)	61-75 баллов (удовлетворительно)	76-85 баллов (хорошо)	86-100 баллов (отлично)
Критерии	Содержание критериев			
Раскрытие проблемы	Проблема не раскрыта. Отсутствуют выводы	Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы	Проблема раскрыта. Проведен анализ проблемы без привлечения дополнительной литературы. Не все выводы сделаны и/или обоснованы	Проблема раскрыта полностью. Проведен анализ проблемы с привлечением дополнительной литературы. Выводы обоснованы
Представление	Представляемая информация логически не связана. Не использованы профессиональные термины	Представляемая информация не систематизирована и/или не последовательна. использовано 1-2 профессиональных термина	Представляемая информация не систематизирована и последовательна. Использовано более 2 профессиональных терминов	Представляемая информация систематизирована, последовательна и логически связана. Использовано более 5 профессиональных терминов
Оформление	Не использованы технологии Power Point. Больше 4 ошибок в представляемой информации	Использованы технологии Power Point частично. 3-4 ошибки в представляемой информации	Использованы технологии Power Point. Не более 2 ошибок в представляемой информации	Широко использованы технологии (Power Point и др.). Отсутствуют ошибки в представляемой информации
Ответы на вопросы	Нет ответов на вопросы	Только ответы на элементарные вопросы	Ответы на вопросы полные и/или частично полные	Ответы на вопросы полные, с привидением примеров и/или пояснений

Критерии оценки (устный ответ)

- 100-85 баллов если ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.
- 85-76 баллов ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать

аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна две неточности в ответе.

- 75-61 балл – оценивается ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.
- 60-50 баллов – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии выставления оценки студенту на экзамене по дисциплине «Информационная безопасность»:

Баллы (рейтинговой оценки)	**Оценка экзамена** (стандартная)	**Требования к сформированным компетенциям** *Дописать оценку в соответствии с компетенциями. Привязать к дисциплине*
	«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач. Знает: Основные понятия документирования процессов создания информационных систем на стадиях жизненного цикла. Основные понятия внедрения, адаптации и настройки

		информационных систем. Владеет: Методами документирования процессов создания информационных систем на стадиях жизненного цикла. Методами внедрения, адаптации и настройки информационных систем. Умеет: документировать процессы создания информационных систем на стадиях жизненного цикла. Осуществлять внедрение, адаптацию и настройку информационных систем.
	«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
	«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
	«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. Не знает: Основные понятия документирования процессов создания информационных систем на стадиях жизненного цикла. Основные понятия внедрения, адаптации и настройки информационных систем. Не владеет: Методами документирования процессов создания информационных систем на стадиях жизненного цикла. Методами внедрения, адаптации и настройки информационных систем. Не умеет: документировать процессы создания информационных систем на стадиях жизненного цикла. Осуществлять внедрение, адаптацию и настройку информационных систем.

Оценочные средства для промежуточной аттестации

Перечень типовых вопросов для итогового контроля:

Вопросы к экзамену

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.

4. Способы и механизмы совершения информационных компьютерных преступлений.

5. Основные параметры и черты информационной компьютерной преступности в России.

6. Компьютерный вирус. Основные виды компьютерных вирусов.

7. Методы защиты от компьютерных вирусов.

8. Типы антивирусных программ.

9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.

10. Основные угрозы компьютерной безопасности при работе в сети Интернет.

11. Виды защищаемой информации.

12. Государственная тайна как особый вид защищаемой информации.

13. Конфиденциальная информация.

14. Система защиты государственной тайны.

15. Правовой режим защиты государственной тайны.

16. Защита интеллектуальной собственности средствами патентного и авторского права.

17. Международное законодательство в области защиты информации.

18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.

19. Симметричные шифры.

20. Ассиметричные шифры.

21. Криптографические протоколы.

22. Криптографические хеш-функции.

23. Электронная подпись.

24. Организационное обеспечение информационной безопасности.

25. Служба безопасности организации.

26. Методы защиты информации от утечки в технических каналах.

27. Инженерная защита и охрана объектов.

28. Настройка основных параметров ASA и межсетевого экрана.

29. Настройка основных параметров, паролей, даты и времени.

30. Настройка внешних и внутренних интерфейсов VLAN.

Тесты для тематической (промежуточной) аттестации:

Методические указания по проведению промежуточной аттестации студентов

Промежуточная аттестация студентов по дисциплине «Информационная безопасность» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Промежуточная аттестация (зачёт) предусмотрена в устной форме с использованием такого оценочного средства, как устный опрос в форме собеседования.

Устный опрос в форме собеседования (УО-1) по раннее известному кругу вопросов позволяет оценить не только знания, но и кругозор обучающегося, навыки логического построения ответов. В ходе собеседования создаются условия, при которых обучающийся имеет возможность показать владение научной лексикой, продемонстрировать, насколько хорошо он ориентируется в предметной области, связанной с данной дисциплиной.

Критерии оценивания решения тестовых заданий

По результатам решения тестовых заданий количество правильно решенных заданий переводится в традиционные оценки посредством применения следующей шкалы:

86% правильно решенных заданий – «отлично»,

75% правильно решенных заданий – «хорошо»,

61% правильно решенных заданий – «удовлетворительно»,

менее 61% «неудовлетворительно».

Оценочные средства для текущей аттестации

1. Кто является основным ответственным за определение уровня классификации информации?

1. Руководитель среднего звена
2. Высшее руководство
3. Владелец
4. Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

1. Сотрудники
2. Хакеры
3. Атакующие
4. Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
3. Улучшить контроль за безопасностью этой информации
4. Снизить уровень классификации этой информации

Что самое главное должно продумать руководство при классификации данных?

1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

2. Необходимый уровень доступности, целостности и конфиденциальности

3. Оценить уровень риска и отменить контрмеры

4. Управление доступом, которое должно защищать данные

4. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

1. Владельцы данных

2. Пользователи

3. Администраторы

4. Руководство

5. Что такое процедура?

1. Правила использования программного и аппаратного обеспечения в компании

2. Пошаговая инструкция по выполнению задачи

3. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

4. Обязательные действия

6. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

1. Поддержка высшего руководства

2. Эффективные защитные меры и методы их внедрения

3. Актуальные и адекватные политики и процедуры безопасности

4. Проведение тренингов по безопасности для всех сотрудников

7. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

2. Когда риски не могут быть приняты во внимание по политическим соображениям

3. Когда необходимые защитные меры слишком сложны

4. Когда стоимость контрмер превышает ценность актива и потенциальные потери

8. Что такое политика безопасности?

1. Пошаговые инструкции по выполнению задач безопасности
2. Общие руководящие требования по достижению определенного уровня безопасности
3. Широкие, высокоуровневые заявления руководства
4. Детализированные документы по обработке инцидентов безопасности

9. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

1. Анализ рисков
2. Анализ затрат / выгоды
3. Результаты ALE
4. Выявление уязвимостей и угроз, являющихся причиной риска

10. Что лучше всего описывает цель расчета ALE?

1. Количественно оценить уровень безопасности среды
2. Оценить возможные потери для каждой контрмеры
3. Количественно оценить затраты / выгоды
4. Оценить потенциальные потери от угрозы в год

11. Тактическое планирование – это:

1. Среднесрочное планирование
2. Долгосрочное планирование
3. Ежедневное планирование
4. Планирование на 6 месяцев

12. Что является определением воздействия (exposure) на безопасность?

1. Нечто, приводящее к ущербу от угрозы
2. Любая потенциальная опасность для информации или систем
3. Любой недостаток или отсутствие информационной безопасности

4. Потенциальные потери от угрозы

13. Эффективная программа безопасности требует сбалансированного применения:

1. Технических и нетехнических методов
2. Контрмер и защитных механизмов
3. Физической безопасности и технических средств защиты
4. Процедур безопасности и шифрования

14. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

1. Внедрение управления механизмами безопасности
2. Классификацию данных после внедрения механизмов безопасности
3. Уровень доверия, обеспечиваемый механизмом безопасности
4. Соотношение затрат / выгод

15. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

1. Только военные имеют настоящую безопасность
2. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
3. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
4. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

16. Как рассчитать остаточный риск?

1. Угрозы х Риски х Ценность актива
2. (Угрозы х Ценность актива х Уязвимости) х Риски
3. SLE х Частоту = ALE
4. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

17. Что из перечисленного не является целью проведения анализа рисков?

1. Делегирование полномочий

2. Количественная оценка воздействия потенциальных угроз

3. Выявление рисков

4. Определение баланса между воздействием риска и стоимостью необходимых контрмер

18. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

1. Поддержка

2. Выполнение анализа рисков

3. Определение цели и границ

4. Делегирование полномочий

19. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

1. Чтобы убедиться, что проводится справедливая оценка

2. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

3. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

4. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

20. Что является наилучшим описанием количественного анализа рисков?

1. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности

2. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков

3. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков

4. Метод, основанный на суждениях и интуиции

21. Почему количественный анализ рисков в чистом виде не достижим?

1. Он достижим и используется

2. Он присваивает уровни критичности. Их сложно перевести в денежный вид.

3. Это связано с точностью количественных элементов

4. Количественные измерения должны применяться к качественным элементам

22. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

1. Много информации нужно собрать и ввести в программу

2. Руководство должно одобрить создание группы

3. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки

4. Множество людей должно одобрить данные

23. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

1. Стандарты

2. Должный процесс (Due process)

3. Должная забота (Due care)

4. Снижение обязательств

24. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

1. Список стандартов, процедур и политик для разработки программы безопасности

2. Текущая версия ISO 17799

3. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

4. Открытый стандарт, определяющий цели контроля

25. Из каких четырех доменов состоит CobiT?

1. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

2. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

3. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка

4. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

26. Что представляет собой стандарт ISO/IEC 27799?

1. Стандарт по защите персональных данных о здоровье

2. Новая версия BS 17799

3. Определения для новой серии ISO 27000

4. Новая версия NIST 800-60

27. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

1. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам

2. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень

3. COSO учитывает корпоративную культуру и разработку политик

4. COSO – это система отказоустойчивости

28. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

1. NIST и OCTAVE являются корпоративными

2. NIST и OCTAVE ориентирован на ИТ

3. AS/NZS ориентирован на ИТ

4. NIST и AS/NZS являются корпоративными

29. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

1. Анализ связующего дерева
2. AS/NZS
3. NIST
4. Анализ сбоев и дефектов

30. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

1. Безопасная OECD
2. ISO\IEC
3. OECD
4. CPTED

Оценочные средства для промежуточной аттестации

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

Разработка аппаратных средств обеспечения правовых данных

Разработка и установка во всех компьютерных правовых сетях журналов учета действий

Разработка и конкретизация правовых нормативных актов обеспечения безопасности

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

Хищение жестких дисков, подключение к сети, инсайдерство

Перехват данных, хищение данных, изменение архитектуры системы

Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

Персональная, корпоративная, государственная

Клиентская, серверная, сетевая

Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

несанкционированного доступа, воздействия в сети

инсайдерства в организации

чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

Компьютерные сети, базы данных

Информационные системы, психологическое состояние пользователей

Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

Искажение, уменьшение объема, перекодировка информации

Техническое вмешательство, выведение из строя оборудования сети

Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

Экономической эффективности системы безопасности

Многоплатформенной реализации системы

Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

руководители, менеджеры, администраторы компаний

органы права, государства, бизнеса

сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

Установление регламента, аудит системы, выявление рисков

Установка новых офисных приложений, смена хостинг-компании

Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:

Неоправданных ограничений при работе в сети (системе)

Рисков безопасности сети, системы

Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

Невозможности миновать защитные средства сети (системы)

Усиления основного звена сети, системы

Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

Усиления защищенности самого незащищенного звена сети (системы)

Перехода в безопасное состояние работы сети, системы

Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

Одноуровневой защиты сети, системы

Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

Компьютерный сбой

Логические закладки («мины»)

Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

Прочитать приложение, если оно не содержит ничего ценного – удалить

Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

Секретность ключа определена секретностью открытого сообщения

Секретность информации определена скоростью передачи данных

Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

Электронно-цифровой преобразователь

Электронно-цифровая подпись

Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

Покупка нелицензионного ПО

Ошибки эксплуатации и неумышленного изменения режима работы системы

Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

Распределенный доступ клиент, отказ оборудования

Моральный износ сети, инсайдерство

Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:

Слабый трафик, информационный обман, вирусы в интернет

Вирусы в сети, логические мины (закладки), информационный перехват

Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

Потерей данных в системе

Изменением формы информации

Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

Целостность

Доступность

Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:

Вероятное событие

Детерминированное (всегда определенное) событие

Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

Регламентированной

Правовой

Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

Программные, технические, организационные, технологические

Серверные, клиентские, спутниковые, наземные

Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

Владелец сети

Администратор сети

Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

Руководств, требований обеспечения необходимого уровня безопасности

Инструкций, алгоритмов поведения пользователя в сети

Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

Аудит, анализ затрат на проведение защитных мер

Аудит, анализ безопасности

Аудит, анализ уязвимостей, риск-ситуаций.

29) Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

30) К внутренним нарушителям информационной безопасности относится:

1. клиенты;
2. пользователи системы;
3. посетители;
4. любые лица, находящиеся внутри контролируемой территории;
5. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.
6. персонал, обслуживающий технические средства.
7. сотрудники отделов разработки и сопровождения ПО;
8. технический персонал, обслуживающий здание.