АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНСТИТУТ МЕЖДУНАРОДНЫХ ЭКОНОМИЧЕСКИХ СВЯЗЕЙ»
INSTITUTE OF INTERNATIONAL ECONOMIC RELATIONS

Принята на заседании
Учёного совета ИМЭС
(протокол от 26 января 2022 г. № 6)

УТВЕРЖДАЮ
Ректор ИМЭС Ю.И. Богомолова
26 января 2022 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0162B6870090AF03B544352CE01F9DE4C7
Владелец: БОГОМОЛОВА ЮЛИЯ ИГОРЕВНА
Действителен: с 20.01.2023 до 20.04.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРОГРАММНЫЕ И АППАРАТНЫЕ СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по направлению подготовки
09.03.02 Информационные системы и технологии

Направленность (профиль)
«Информационные системы и сетевые технологии»

Москва – 2022

I. АННОТАЦИЯ К ДИСЦИПЛИНЕ

Рабочая программа дисциплины «Программные и аппаратные средства информационной безопасности» (ПиАСИБ) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденным приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 926.

Изучение дисциплины «Программные и аппаратные средства информационной безопасности» ориентировано на получение обучающимися знаний в области защиты информации с использованием соответствующих программных и аппаратных средств. Также дисциплина развивает ряд практических навыков и умений, позволяющих студентам осуществлять установку и настройку аппаратных и программных средств защиты информации, формировать комплекс средств защиты информации от различных видов угроз таких как сетевые атаки, вредоносное программное обеспечение и несанкционированный доступ к данным.

Место дисциплины в структуре образовательной программы

Настоящая дисциплина включена в учебные планы по программам подготовки бакалавров по направлению 09.03.02 Информационные системы и технологии и входит часть, формируемую участниками образовательных отношений, Блока 1.

Дисциплина изучается на 1 курсе в 1 семестре.

Цель и задачи дисциплины

Цель изучения дисциплины **–** формирование у обучающихся необходимых компетенций для успешного освоения образовательной программы, в частности, ознакомление с принципами работы программных и аппаратных средств, используемых для защиты информации, а также с конкретными образцами ПиАСИБ.

Задачи изучения дисциплины:

- сформировать знание основ архитектуры ИС, бизнес-процессов, моделей их проектирования и анализа;
- сформировать умение осуществлять анализ и реинжиниринг бизнес-процессов в организациях различных форм собственности, определение перечня программных и аппаратных средств для создания архитектуры ИС;
- формирование практического опыта разработки спецификации архитектуры ИС;
- сформировать знание основ информационных систем, их классификации, состав информационных систем, их создания, сопровождения, организации, управления и модификации;
- формирование умения осуществлять выбор инструментальных программно-аппаратных средств для проектирования информационных

систем и применять современные технологии описания бизнес-процессов;

- сформировать практический опыт использования технологий проектирования, отладки, проверки работоспособности, навыками создания (модификации) и сопровождения ИС; анализа и управления бизнес-процессами для повышения эффективности деятельности организаций.

2. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций, предусмотренных образовательной программой.

Результаты освоения ООП (содержание компетенций)	**Код компе-тенции**	**Код и наименование индикатора достижения компетенций**	**Перечень планируемых результатов обучения по дисциплине**			**Формы образовательной деятельности**
			выпускник должен знать	**выпускник должен уметь**	**выпускник должен иметь практический опыт**	
Способность разрабатывать архитектуру ИС, включая сбор исходных данных, анализ бизнес-процессов и коммуникацию с заказчиком в организациях различных форм собственности	**ПК-1**	**ПК-1.1** Собирает исходные данные у заказчика, описывает и моделирует на их основе бизнес-процессы, согласует результат с заказчиком	функции сетевого экранирования; классификацию, возможности и параметры межсетевых экранов; принципы фильтрации сетевого трафика; функции и технологии организации, защищенных виртуальных частных сетей (VPN); разновидности сетевых атак; средства обнаружения и отражения сетевых атак	оценивать возможности ПиАСИБ в контексте политики информационной безопасности организации	проведения анализа технико-экономических характеристик образцов ПиАСИБ для подготовки предложений об эксплуатации данных средств на всех этапах их жизненного цикла ИС	Контактная работа: Лекции Лабораторные практикумы Самостоятельная работа
		ПК-1.2 Проводит анализ и реинжиниринг бизнес-процессов в организациях различных форм собственности	средства анализа защищенности ПК. способы организации и построения защищенных виртуальных частных сетей (VPN)	проводить сравнительный анализ и выбор ПиАСИБ исходя из условий поставленной задачи; осуществлять установку, настройку и эксплуатацию ПиАСИБ; формировать политику использования выбранных ПиАСИБ	модернизации программной и технической архитектуры организации с целью обеспечения информационной безопасности и защиты данных	
		ПК-1.3 Разрабатывает спецификацию архитектуры ИС	методы и средства разработки спецификации архитектуры ИС с учетом	разрабатывать спецификацию по установке, настройке и эксплуатации ПиАСИБ	составления спецификаций по модернизации программной и технической архитектуры	

Результаты освоения ООП (содержание компетенций)	Код компе-тенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	
			ПиАСИБ		организации с целью обеспечения информационной безопасности и защиты данных	
Способность к проектированию, отладке, проверке работоспособности, созданию (модификации) и сопровождению информационных систем (ИС), автоматизирующих задачи организационного управления и бизнес-процессы с целью повышения эффективности деятельности организаций - пользователей ИС	**ПК-2**	**ПК-2.1** Разрабатывает и верифицирует структуру программного кода и баз данных ИС, автоматизирующих задачи организационного управления и бизнес-процессы организаций	средства криптографической защиты данных; принципы использования электронно-цифровой подписи (ЭЦП)	оценивать возможности средств криптографической защиты данных	использования средств криптографической защиты данных	Контактная работа: Лекции Лабораторные практикумы Самостоятельная работа
		ПК-2.2 Согласовывает необходимость внесения изменений, обеспечивает и контролирует соответствие разработанного кода и процесса кодирования на языках программирования принятым в организации или проекте стандартам и технологиям	принципы и средства разграничения прав доступа в ОС; принципы и средства ролевого управления правами доступа в ОС	проводить сравнительный анализ и выбор средств криптографической защиты данных исходя из условий поставленной задачи; определять и настраивать групповые политики безопасности в ОС семейства Windows	модернизации программной и технической архитектуры путем включения средств криптографической защиты данных	
		ПК-2.3 Разрабатывает, верифицирует и модифицирует пользовательские интерфейсы с целью повышения эффективности деятельности организаций - пользователей	стандарты шифрования; средства криптографической защиты данных	оценивать возможности средств криптографической защиты данных; настраивать систему аудита событий в ОС семейства Windows; настраивать встроенные средства обеспечения безопасности ОС семейства Windows; настраивать	администрирования средств обеспечения безопасности ОС семейства Windows; ролевого управления доступом в ОС семейства Windows	

Результаты освоения ООП (содержание компетенций)	Код компе-тенции	Код и наименование индикатора достижения компетенций	Перечень планируемых результатов обучения по дисциплине			Формы образовательной деятельности
			выпускник должен знать	выпускник должен уметь	выпускник должен иметь практический опыт	
				архивирование данных компьютера и производить их восстановление из архива; определять и настраивать групповые политики безопасности в ОС семейства Windows		

3. ТЕМАТИЧЕСКИЙ ПЛАН

Наименование тем	Контактная работа обучающихся с преподавателем (по видам учебных занятий)									Самостоятельная работа обучающихся	ТКУ / балл Форма ПА
	Лекции	Семинары	Практикум по решению задач	Ситуационный практикум	Мастер-класс	Лабораторный практикум	Тренинг	Дидактическая игра	Из них в форме практической полготовки		
Очная форма											
Тема 1. Средства идентификации и аутентификации пользователей.	2					4				7	Отчет по лабораторному практикуму/10 Реферат/10
Тема 2. Криптографическая защита информации.	2					4				7	Отчет по лабораторному практикуму/10
Тема 3. Безопасность операционных систем.	2					4				7	Отчет по лабораторному практикуму/10 Реферат/10
Тема 4. Технологии межсетевых экранов.	2					4				7	Отчет по лабораторному практикуму/10
Тема 5. Основы технологии виртуальных защищенных сетей.	4					8				7	Отчет по лабораторному практикуму/10
Тема 6. Технологии обнаружения атак.	4					8				8	Отчет по лабораторному практикуму/10
Тема 7. Технологии защиты от вирусов.	3					6				8	Отчет по лабораторному практикуму/10 Эссе/10
Всего:	**19**					**38**				**51**	**100**
Контроль, час	**0**										**Зачёт**
Объем дисциплины (в академических часах)	**108**										
Объем дисциплины (в зачетных единицах)	**3**										

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Тема 1. Средства идентификации и аутентификации пользователей

Основные понятия: идентификация, аутентификация, авторизация. Аутентификация на основе многоразовых паролей. Аутентификация на основе одноразовых паролей. Аутентификация на основе PIN-кода. Строгая аутентификация. Аутентификация с общим ключом. Особенности применения внешних носителей ключевой информации для идентификации и аутентификации. Программные и аппаратные средства идентификации и аутентификации.

Тема 2. Криптографическая защита информации

Основные понятия криптографии. Криптографическая система. История криптографии. Классификация криптоалгоритмов. Симметричные системы шифрования. Алгоритм шифрования DES. Стандарт шифрования ГОСТ 28147-89. Асимметричное шифрование. Электронная цифровая подпись (ЭЦП). Хэширование. Программные и аппаратные средства криптографической защиты данных.

Тема 3. Безопасность операционных систем

Угрозы безопасности ОС. Механизмы защиты ОС. Разграничение доступа в ОС. Ролевое управление доступом. Реализация ролевого управления доступом. Аудит событий безопасности в ОС. Защитные механизмы ОС семейства Windows и Unix.

Тема 4. Технологии межсетевых экранов

Функции сетевого экранирования. Классификация МЭ. Фильтрация трафика. Сервисы межсетевого экранирования. Программные и аппаратные средства сетевого экранирования.

Тема 5. Основы технологии виртуальных защищенных сетей.

Функции технологии виртуальных защищенных сетей (VPN). Варианты организации VPN. Варианты построения VPN. Программные и аппаратные средства создания защищенных VPN. Виртуальные локальные сети.

Тема 6. Технологии обнаружения атак

Противодействие сетевым атакам. Защита информации с помощью средств анализа защищённости. Защита информации с помощью систем обнаружения атак. Разновидности сетевых атак. Программные средства обнаружения и отражения сетевых атак.

Тема 7. Технологии защиты от вирусов

Вредоносный программный код. Организация эшелонной защиты. Компоненты защиты от вредоносного ПО. Признаки заражения

компьютера. Действия при заражении компьютера. Разработчики антивирусного программного обеспечения. Программные средства защиты от компьютерных вирусов. Безопасность в социальных сетях.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

В процессе изучения данной дисциплины используются такие виды учебной работы, как лекция, лабораторный практикум, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков использования профессиональной лексики, закрепление практических профессиональных компетенций, поощрение интеллектуальных инициатив.

Методические указания для обучающихся при работе над конспектом лекций во время проведения лекции

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к экзамену.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы по лекции подытоживают размышления преподавателя по учебным вопросам. Формулируются они кратко и лаконично, их целесообразно записывать. В конце лекции обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

Методические указания для обучающихся по выполнению лабораторных практикумов

Лабораторные практикумы выполняются в соответствии с рабочим учебным планом при последовательном изучении тем дисциплины.

Порядок проведения практикума.

1. Получение задания и рекомендаций к выполнению практикума.
2. Настройка инструментальных средств, необходимых для выполнения практикума.
3. Выполнение заданий практикума.
4. Подготовка отчета в соответствии с требованиями.

5. Сдача отчета преподавателю.

В ходе выполнения практикума необходимо следовать технологическим инструкциям, использовать материал лекций, рекомендованных учебников, источников интернета, активно использовать помощь преподавателя на занятии.

Требования к оформлению результатов практикумов (отчет)

При подготовке отчета: изложение материала должно идти в логической последовательности, отсутствие грамматических и синтаксических ошибок, шрифт Times New Roman, размер – 14, выравнивание по ширине, отступ первой строки – 1,25, междустрочный интервал – 1,5, правильное оформление рисунков (подпись, ссылка на рисунок в тексте).

При подготовке презентации: строгий дизайн, минимум текстовых элементов, четкость формулировок, отсутствие грамматических и синтаксических ошибок, воспринимаемая графика, умеренная анимация.

Методические указания для обучающихся по организации самостоятельной работы

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем/вопросов учебной дисциплины.

Самостоятельная работа является обязательной для каждого обучающегося, ее объем по дисциплине определяется учебным планом.

При самостоятельной работе обучающиеся взаимодействуют с рекомендованными материалами при минимальном участии преподавателя.

Работа с литературой (конспектирование)

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Изучая материал по учебной книге (учебнику, учебному пособию, монографии, и др.), следует переходить к следующему вопросу только после полного уяснения предыдущего, фиксируя выводы и вычисления (конспектируя), в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода.

Особое внимание обучающийся должен обратить на определение основных понятий курса. Надо подробно разбирать примеры, которые поясняют определения. Полезно составлять опорные конспекты.

Выводы, полученные в результате изучения учебной литературы, рекомендуется в конспекте выделять, чтобы при перечитывании материала они лучше запоминались.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса.

Вопросы, которые вызывают у обучающегося затруднение при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Реферат

Подготовка рефератов направлена на развитие и закрепление у обучающихся навыков самостоятельного глубокого, творческого и всестороннего анализа научной, методической и другой литературы по актуальным проблемам дисциплины; на выработку навыков и умений грамотно и убедительно излагать материал, четко формулировать теоретические обобщения, выводы и практические рекомендации.

Рефераты должны отвечать высоким квалификационным требованиям в отношении научности содержания и оформления.

Темы рефератов, как правило, посвящены рассмотрению одной проблемы. Объем реферата может быть от 12 до 15 страниц машинописного текста, отпечатанного через 1,5 интервала, а на компьютере через 1 интервал (список литературы и приложения в объем не входят).

Текстовая часть работы состоит из введения, основной части и заключения.

Во введении обучающийся кратко обосновывает актуальность избранной темы реферата, раскрывает конкретные цели и задачи, которые он собирается решить в ходе своего небольшого исследования.

В основной части подробно раскрывается содержание вопроса (вопросов) темы.

В заключении кратко должны быть сформулированы полученные результаты исследования и даны выводы. Кроме того, заключение может включать предложения автора, в том числе и по дальнейшему изучению заинтересовавшей его проблемы.

В список литературы (источников и литературы) обучающийся включает только те документы, которые он использовал при написании реферата.

В приложении (приложения) к реферату могут выноситься таблицы, графики, схемы и другие вспомогательные материалы, на которые имеются ссылки в тексте реферата.

Эссе

Эссе - это самостоятельная письменная работа на тему, предложенную преподавателем. Цель эссе состоит в развитии навыков самостоятельного творческого мышления и письменного изложения собственных мыслей.

Эссе должно содержать: четкое изложение сути поставленной проблемы, включать самостоятельно проведенный анализ этой проблемы с использованием концепций и аналитического инструментария, рассматриваемого в рамках дисциплины, выводы, обобщающие авторскую позицию по поставленной проблеме. В зависимости от специфики дисциплины формы эссе могут значительно дифференцироваться.

Структура эссе.

1. Титульный лист
2. Введение - суть и обоснование выбора данной темы, состоит из ряда компонентов, связанных логически и стилистически; На этом этапе очень важно правильно сформулировать вопрос, на который вы собираетесь найти ответ в ходе своего исследования.

При работе над введением могут помочь ответы на следующие вопросы: «Надо ли давать определения терминам, прозвучавшим в теме эссе?», «Почему тема, которую я раскрываю, является важной в настоящий момент?», «Какие понятия будут вовлечены в мои рассуждения по теме?», «Могу ли я разделить тему на несколько более мелких подтем?».

3. Основная часть - теоретические основы выбранной проблемы и изложение основного вопроса.

Данная часть предполагает развитие аргументации и анализа, а также обоснование их, исходя из имеющихся данных, других аргументов и позиций по этому вопросу. В этом заключается основное содержание эссе и это представляет собой главную трудность. Поэтому важное значение имеют подзаголовки, на основе которых осуществляется структурирование аргументации; именно здесь необходимо обосновать (логически, используя данные или строгие рассуждения) предлагаемую аргументацию/анализ. Там, где это необходимо, в качестве аналитического инструмента можно использовать графики, диаграммы и таблицы.

В зависимости от поставленного вопроса анализ проводится на основе следующих категорий:

Причина — следствие, общее — особенное, форма — содержание, часть — целое, постоянство — изменчивость.

Хорошо проверенный способ построения любого эссе — использование подзаголовков для обозначения ключевых моментов аргументированного изложения: это помогает посмотреть на то, что предполагается. Такой подход поможет следовать точно определенной цели в данном исследовании. Эффективное использование подзаголовков - не только обозначение основных пунктов, которые необходимо осветить. Их последовательность может также свидетельствовать о наличии или отсутствии логичности в освещении темы.

4. Заключение - обобщения и аргументированные выводы по теме с указанием области ее применения и т.д. Методы, рекомендуемые для составления заключения: повторение, иллюстрация, цитата, впечатляющее утверждение. Заключение может содержать такой очень важный, дополняющий эссе элемент, как указание на применение исследования, не исключая взаимосвязи с другими проблемами.

Навигация для обучающихся по самостоятельной работе в рамках изучения дисциплины

Наименование темы	Вопросы, вынесенные на самостоятельное изучение	Формы самостоятельной работы	Форма контроля
Тема 1. Средства идентификации и аутентификации пользователей.	Особенности применения внешних носителей ключевой информации для идентификации и аутентификации. Программные и аппаратные средства идентификации и аутентификации.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму Подготовка реферата	Реферат Отчет по лабораторному практикуму
Тема 2. Криптографическая защита информации.	Хэширование. Программные и аппаратные средства криптографической защиты данных.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 3. Безопасность операционных систем.	Аудит событий безопасности в ОС. Защитные механизмы ОС семейства Windows и Unix.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму Подготовка реферата	Реферат Отчет по лабораторному практикуму
Тема 4. Технологии межсетевых экранов.	Сервисы межсетевого экранирования**.** Программные и аппаратные средства сетевого экранирования.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 5. Основы технологии виртуальных защищенных сетей.	Программные и аппаратные средства создания защищенных VPN. Виртуальные локальные сети.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму

Наименование темы	Вопросы, вынесенные на самостоятельное изучение	Формы самостоятельной работы	Форма контроля
Тема 6. Технологии обнаружения атак.	Разновидности сетевых атак. Программные средства обнаружения и отражения сетевых атак.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму	Отчет по лабораторному практикуму
Тема 7. Технологии защиты от вирусов.	Разработчики антивирусного программного обеспечения. Программные средства защиты от компьютерных вирусов.	Работа с литературой, включая ЭБС, источниками в сети Internet Подготовка к лабораторному практикуму, подготовка отчета по практикуму Подготовка эссе	Отчет по л лабораторному практикуму Эссе

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Перечень основной и дополнительной литературы

Основная литература:

1. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

2. Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: http://biblioclub.ru/

Дополнительная литература

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/;

3. Шилов, А.К. Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ, Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 121 с. : ил. – Режим доступа: по

подписке. – URL: http://biblioclub.ru/

4. Смирнов, В.И. Защита информации: лабораторный практикум / В.И. Смирнов ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2017. – 67 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/;

5. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/.

6.2. Перечень ресурсов информационно-коммуникационной сети «Интернет»

№	Наименование ресурса	Ссылка
1.	Ассоциация по вопросам защиты информации	http://bis-expert.ru/
2.	Специализированный сайт по тематике информационной безопасности, противодействие вредоносному программному коду, использование утилиты AVZ	http://z-oleg.com/index.php
3	Официальный сайт Institute of Electrical and Electronics Engineers (IEEE)	https://www.ieee.org/
4	Официальный сайт компании Infowatch	http://www.infowatch.ru/
5	Официальный сайт Лаборатории Касперского	http://www.kaspersky.ru/

6.3. Описание материально-технической базы

Материально-техническое обеспечение дисциплины включает в себя:

Учебная аудитория (Лаборатория информационно-коммуникационных технологий), оборудованная:

комплекты специализированной учебной мебели, мультимедийный проектор, экран, доска классная, принтер, компьютер преподавателя и компьютеры обучающихся с выходом в сеть «Интернет», доступом в электронную информационно-образовательную среду.

Помещение для самостоятельной работы обучающихся – аудитория, оборудованная:

комплекты специализированной учебной мебели, мультимедийный проектор, экран, доска классная, компьютеры с выходом в сеть «Интернет» и доступом в электронную информационно-образовательную среду.

6.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, в том числе комплект лицензионного программного обеспечения, электронно-библиотечные системы, современные профессиональные базы данных и информационные справочные системы

Обучающиеся обеспечены доступом к электронной информационно-образовательной среде из любой точки, в которой имеется доступ к сети «Интернет», как на территории организации, так и вне ее.

лицензионное программное обеспечение:

- Windows (зарубежное, возмездное);
- MS Office (зарубежное, возмездное);
- Adobe Acrobat Reader (зарубежное, свободно распространяемое);
- КонсультантПлюс: «КонсультантПлюс: Студент» (российское, свободно распространяемое);
- 7-zip – архиватор (зарубежное, свободно распространяемое);
- Comodo Internet Security (зарубежное, свободно распространяемое);
- MySQL for Windows – реляционная система управления базами данных (зарубежное, свободно распространяемое);
- Apache NetBeans – свободная интегрированная среда разработки приложений (IDE) на языках программирования Java, Python, PHP, JavaScript, C, C++, Ада и ряда других (зарубежное, свободно распространяемое);
- Android Studio – разработка мобильных приложений (зарубежное, свободно распространяемое)

электронно-библиотечная система:

- Электронная библиотечная система (ЭБС) «Университетская библиотека ONLINE» http://biblioclub.ru/.
- Образовательная платформа «Юрайт». Для вузов и ссузов. Электронная библиотечная система (ЭБС) https://urait.ru/

современные профессиональные баз данных:

- Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru.
- Портал Единое окно доступа к образовательным ресурсам http://window.edu.ru/

информационные справочные системы:

- Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru.
- Компьютерная справочная правовая система «КонсультантПлюс» (http://www.consultant.ru/).

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание оценочных средств для проведения текущего контроля успеваемости в процессе освоения дисциплины

№ п/п	Форма учебного занятия, по которому проводится ТКУ/ оценочное средство	Шкала и критерии оценки, балл
1.	Лабораторный практикум	10-9 – работа и отчет выполнены в срок, самостоятельно, правильно выбрано и использовано инфокоммуникационное оборудование, серверы и программное обеспечение, необходимые выводы, хорошо аргументированы, даны исчерпывающие ответы на все поставленные вопросы; 8-7 – работа и отчет выполнены в срок, самостоятельно, правильно выбрано и использовано инфокоммуникационное оборудование, серверы и программное обеспечение, необходимые выводы сделаны частично, хорошо аргументированы, даны ответы на все поставленные вопросы; 6 – работа и отчет выполнены в срок, самостоятельно, правильно выбрано и использовано инфокоммуникационное оборудование, серверы и программное обеспечение, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 5 – обучающийся подготовил работу и отчет самостоятельно, но присутствуют неточности или неполнота в описании выбранных программно-аппаратных средств, выводы сделаны частично, слабо аргументированы, даны ответы не на все вопросы; 4 – обучающийся подготовил работу и отчет несамостоятельно или не завершил в срок, описание спецификации содержит незначительные ошибки, выводы и ответы на вопросы отсутствуют.
2.	Эссе	10 – грамотное использование компьютерной терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 6 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 3 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения.
3.	Реферат	10 – грамотное использование компьютерной терминологии, свободное изложение рассматриваемой проблемы, логичность и обоснованность выводов; 6 – грамотное использование компьютерной терминологии, частично верные суждения в рамках рассматриваемой темы, выводы недостаточно обоснованы; 3 – грамотное использование компьютерной терминологии, способность видения существующей проблемы, необоснованность выводов, неполнота аргументации собственной точки зрения.

Типовые контрольные задания или иные материалы в рамках текущего контроля успеваемости

Типовые задания к лабораторным практикумам

Лабораторный практикум № 1. Средства идентификации и аутентификации пользователей.

Часть 1.

Раздел 1.

Разработайте проект технической архитектуры организации (например, с использованием пакета MS Visio), отвечающий следующим требованиям в соответствии с вашим вариантом. Каждое устройство должно быть подписано. Подпись должна содержать название устройства, производителя и модель.

Вариант 1.

1. терминальный сервер;
2. сервер базы данных;
3. сервер приложений;
4. обеспечение защищенного выхода в Internet с любого компьютера локальной сети;
5. не менее двух самостоятельных сегментов сети, взаимодействующих друг с другом;
6. количество рабочих станций – произвольное;
7. подключение не менее одного устройства через беспроводной интерфейс;
8. возможность подключения к данной сети мобильных устройств и ноутбуков через WiFi;
9. не менее одного устройства для обеспечения внутренней и внешней телефонной связи.

Вариант 2.

1) файл-сервер;
2) принт-сервер;
3) контроллер домена (DNS) – сервер;
4) обеспечение защищенного выхода в Internet с любого компьютера локальной сети;
5) не менее двух самостоятельных сегментов сети, взаимодействующих друг с другом;
6) количество рабочих станций – произвольное;
7) подключение не менее одного устройства через беспроводной интерфейс;
8) возможность подключения к данной сети мобильных устройств и ноутбуков через WiFi;
9) не менее одного устройства для обеспечения внутренней и внешней телефонной связи.

Вариант 3.

1) сервер защиты данных;
2) почтовый сервер;
3) сервер удаленного доступа;
4) обеспечение защищенного выхода в Internet с любого компьютера локальной сети;

5) возможность подключения удаленных устройств;

6) количество рабочих станций – произвольное;

7) возможность подключения к данной сети мобильных устройств и ноутбуков через WiFi;

8) не менее одного устройства для обеспечения внутренней и внешней телефонной связи;

9) не менее одного сетевого принтера.

Рекомендуемая последовательность выполнения задания:

1) определить способ размещения серверов – в стойке или каждый самостоятельно;

2) сделать первый вариант технической архитектуры, разместив серверы, рабочие станции и основное коммуникационное оборудование;

3) определить перечень дополнительного коммуникационного оборудования;

4) сделать второй вариант технической архитектуры, добавив дополнительное коммуникационное оборудование и подключаемые с его помощью устройства;

5) определить перечень устройств защиты данных и удаленного доступа;

6) сделать финальный вариант технической архитектуры, добавив устройства защиты данных и удаленного доступа.

Раздел 2.

Разработайте проект программной архитектуры организации (например, с использованием пакета MS Visio), соответствующий технической архитектуре, разработанной в Разделе 1. Обратите внимание на то, что обе архитектуры должны полностью соответствовать друг другу. При разработке необходимо использовать актуальное программное обеспечение и совместимые протоколы передачи данных.

Проект должен отражать реальные устройства и программное обеспечение, выбранные вами.

Часть 2.

Изучить характеристики аппаратных и программных средств идентификации и аутентификации (СИА).

1. Проанализировать достоинства и недостатки представителей классов (подклассов) СИА.
2. Результаты анализа внести в таблицу.
3. Ответить на вопросы:

- Какие факторы влияют на надежность работы СИА?
- В чем принципиальное отличие статической и динамической биометрии?
- В чем особенность гибридных смарт-карт?
- Какие способы используются для предотвращения доступа к

информации посторонних лиц в случае несанкционированного овладения ими средствами идентификации и авторизации?

- Что такое интеллектуальная карта?

Внести изменения в разработанную программную и техническую архитектуру добавив выбранные средства идентификации и аутентификации.

ВНИМАНИЕ! Перед внесением изменений сохранить на отдельных листах первоначальные проекты технической и программной архитектур, разработанные в ходе выполнения части 1.

Лабораторный практикум № 2. Криптографическая защита информации

Часть 1.

Выполняется в парах.

1. Установить программы Crypton API и Crypton Emulator компании АНКАД.
2. Провести шифрование данных и отправить зашифрованные пакеты напарнику.
3. Провести расшифровку пакетов, полученных от напарника.

Часть 2.

1. Изучить характеристики аппаратных и программных средств шифрования данных.
2. Проанализировать достоинства и недостатки представителей классов (подклассов) средств шифрования данных.

Внести изменения в разработанную программную и техническую архитектуру, добавив выбранные средства шифрования данных.

Лабораторный практикум № 3. Безопасность операционных систем

1. В операционной системе Windows 7 и выше создайте учетную запись пользователя, установите для нее логин, пароль и права доступа к информационным ресурсам.
2. Под учетной записью администратора проведите настройку систем безопасности, в том числе локальной политики безопасности, автоматического обновления операционной системы, архивирования данных, фильтрации трафика и так далее.

Лабораторный практикум № 4. Технологии межсетевых экранов

1. Используя ресурсы сети Internet выберете два программных и два аппаратных межсетевых экрана (МЭ).
2. Изучите функциональные возможности, системные требования, особенности инсталляции и сопровождения данных МЭ.

3. Проведите сравнительный анализ данных МЭ.

Внесите изменения в разработанную программную и техническую архитектуру, добавив выбранный межсетевой экран.

Лабораторный практикум № 5. Основы технологии виртуальных защищенных сетей

1. Используя ресурсы сети Internet выберите по два программных и аппаратных средства реализации защищенного VPN соединения.
2. Изучите функциональные возможности, системные требования, особенности инсталляции и сопровождения данных средств.
3. Проведите сравнительный анализ данных средств.

Внесите изменения в разработанную программную и техническую архитектуру, добавив выбранные средства реализации защищенной VPN.

Лабораторный практикум № 6. Технологии обнаружения атак

1. Используя ресурсы сети Internet выберете два средства обнаружения и отражения сетевых атак (СОиОСА).
2. Изучите функциональные возможности, системные требования, особенности инсталляции и сопровождения данных СОиОСА.
3. Проведите сравнительный анализ данных СОиОСА.

Внесите изменения в разработанную программную и техническую архитектуру, добавив выбранные средства СОиОСА.

Лабораторный практикум № 7. Технологии защиты от вирусов

Часть 1.

1. Запустите (откройте) антивирусную программу, например, AVZ, 360 Total Security.
2. Проведите настройку системы (эвристический анализ, уровень безопасности, алгоритмы действий с обнаруженным вредоносным программным кодом).
3. Проведите сканирование жесткого диска и flash накопителя на предмет поиска вирусов.

Часть 2.

1. Используя ресурсы сети Internet выберете два средства защиты от вредоносного программного кода.
2. Изучите функциональные возможности, системные требования, особенности инсталляции и сопровождения данных средств.
3. Проведите сравнительный анализ данных средств.

Внесите изменения в разработанную программную и техническую архитектуру, добавив выбранные средства защиты от вредоносного программного кода.

<u>Примерные темы рефератов</u>

по теме 1:

1. USB-ключи и смарт-карты eToken – персональное средство аутентификации и защищенного хранения данных.
2. JaCarta – новое поколение смарт-карт, USB- и Secure MicroSD-токенов для строгой аутентификации, электронной подписи и безопасного хранения ключей, цифровых сертификатов.
3. Смарт-карт ридеры — устройства, обеспечивающие считывание информации со смарт-карт и запись на них необходимых данных.
4. «Антифрод-терминал» – защита от атак киберпреступников при работе пользователей с защищёнными сервисами через Интернет с использованием смарт-карт.
5. JaCarta Management System (JMS) – система управления, полноценно поддерживающая новое поколение средств аутентификации и электронной подписи JaCarta, а также eToken.
6. SafeNet Authentication Manager (SAM) — программное решение для управления инфраструктурой аутентификации в масштабах предприятия.
7. Secret Disk Enterprise – корпоративная система защиты конфиденциальной информации с централизованным управлением.
8. Secret Disk Server NG – комплекс защиты конфиденциальной информации и персональных данных на сервере от несанкционированного доступа, копирования, повреждения, кражи или неправомерного изъятия.
9. Secret Disk 4 – Система защиты конфиденциальной информации от несанкционированного доступа, копирования, повреждения, кражи или неправомерного изъятия.
10. eToken PKI Client – набор драйверов и утилит, обеспечивающих работу USB-ключей и смарт-карт eToken.
11. eToken PKI Client – набор драйверов и утилит, обеспечивающих работу USB-ключей и смарт-карт eToken.
12. Электронные ключи eToken PRO (Java) – персональное средство аутентификации и защищенного хранения пользовательских данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронно-цифровой подписью (ЭЦП).
13. eToken Network Logon – средство управления паролями при работе на компьютерах под управлением Microsoft Windows.
14. Средства аутентификации по отпечаткам пальцев.
15. Средства аутентификации по радужной оболочке глаза.
16. Средства аутентификации по сетчатке глаза.
17. Средства аутентификации по геометрии лица или руки.
18. Средства аутентификации по термограмме лица.
19. Средства аутентификации по голосу.

по теме 3:

1. Защитные механизмы ОС Windows Server 2008.
2. Защитные механизмы ОС Windows Small Business Server 2008.
3. Защитные механизмы ОС Windows 7.
4. Защитные механизмы ОС Windows 8.

5. Защитные механизмы ОС Windows 8.1.
6. Защитные механизмы ОС Windows Server 2008 R2.
7. Защитные механизмы ОС Windows Home Server 2011.
8. Защитные механизмы ОС Windows Server 2012.
9. Защитные механизмы ОС Windows Server 2012 R2.
10. Защитные механизмы ОС Linux Ubuntu.
11. Защитные механизмы ОС Linux Red Hat.
12. Защитные механизмы ОС Debian GNU/Linux.
13. Защитные механизмы ОС FreeBSD.
14. Защитные механизмы ОС Linux Mint.
15. Защитные механизмы ОС Linux openSUSE.
16. Защитные механизмы ОС macOS

Примерные темы эссе

1. Kaspersky Internet Security.
2. Kaspersky CRYSTAL.
3. Kaspersky Anti-Virus.
4. Dr.Web Security Space.
5. Антивирус Dr.Web.
6. Dr.Web Бастион.
7. ESET NOD32 Smart Security.
8. ESET NOD32 TITAN.
9. ESET NOD32 Cyber Security Pro.
10. ESET NOD32 START PACK.
11. ESET NOD32 Антивирус.
12. Norton AntiVirus.
13. Norton Internet Security.
14. Norton 360.
15. Symantec Endpoint Protection.
16. Symantec Endpoint Protection Small Business Edition.
17. Symantec Protection Suite Small Business Edition.

7.2. Описание оценочных средств для проведения промежуточной аттестации

Промежуточная аттестация по дисциплине проводится в форме зачёта.

Процедура оценивания	Шкала и критерии оценки, балл
Зачет представляет собой выполнение обучающимся заданий билета, включающего в себя. Задание №1 – теоретический вопрос на знание базовых понятий предметной области дисциплины, а также позволяющий оценить степень	Выполнение обучающимся заданий билета оценивается по следующей балльной шкале: Задание 1: 0-30 баллов Задание 2: 0-30 баллов Задание 3: 0-40 баллов **«Зачтено»** – 90-100 – ответ правильный, логически

Процедура оценивания	Шкала и критерии оценки, балл
владения обучающегося принципами предметной области дисциплины, понимание их особенностей и взаимосвязи между ними; Задание №2 – задание на анализ ситуации из предметной области дисциплины и выявление способности обучающегося выбирать и применять соответствующие принципы и методы решения практических проблем, близких к профессиональной деятельности; Задания №3 – задания на проверку умений и навыков, полученных в результате освоения дисциплины	выстроен, использована профессиональная терминология. Задания решены правильно. Обучающийся правильно интерпретирует полученный результат. – 70 -89 – ответ в целом правильный, логически выстроен, использована профессиональная терминология. Ход решения заданий правильный, ответ неверный. Обучающийся в целом правильно интерпретирует полученный результат. – 50 - 69 – ответ в основном правильный, логически выстроен, использована профессиональная терминология. Задание решено частично. **«Не зачтено»** – менее 50 – ответы на теоретическую часть неправильные или неполные. Задания не решены.

Типовые задания для проведения промежуточной аттестации обучающихся

Задания на знания

1. Содержание основных этапов организации доступа к информации: идентификация, аутентификация, авторизация.
2. Порядок организации и средства реализации аутентификации на основе многоразовых и одноразовых паролей.
3. Порядок организации и средства реализации аутентификации на основе PIN-кода.
4. Порядок организации и средства реализации строгой аутентификации.
5. Порядок организации и средства реализации аутентификации с общим ключом.
6. Криптография как наука и сфера практической деятельности. Основные этапы развития криптографии, соответствующие примеры систем шифрования.
7. Структура, назначение и порядок работы основных элементов криптографической системы. Перечень, назначение и логика работы криптоалгоритмов.
8. Алгоритм работы и способы реализации симметричных и асимметричных систем шифрования.
9. Принцип работы и основные параметры алгоритм шифрования DES. Принцип работы и основные параметры стандарта шифрования ГОСТ 28147-89.
10. Алгоритм работы и способы реализации хэширования. Назначение, возможности и практическое использование электронной цифровой подписи (ЭЦП).
11. Типы, источники и способы реализации основанных угроз

операционных систем. Перечень, возможности и порядок работы основных встроенных средств защиты операционных систем.

12. Способы и средства разграничения доступа в операционных системах.

13. Порядок организации и практическая реализация ролевого управления доступом в операционных системах.

14. Назначение, возможности, средства и способы реализации функций сетевого экранирования.

15. Назначение, возможности, средства и способы реализации межсетевых экранов.

16. Назначение, возможности и способы реализации средств фильтрации сетевого трафика.

17. Назначение и возможности технологии виртуальных защищенных сетей (VPN). Принципы работы и протоколы туннелирования.

18. Способы организации и средства реализации виртуальных защищенных сетей (VPN) .

19. Виды и способы реализации сетевых атак. Средства защиты от сетевых атак.

20. Перечень, возможности и порядок использования средств анализа защищённости для защиты от сетевых атак. Преимущества и недостатки средств анализа защищённости.

21. Типы, возможности и порядок использования средств обнаружения сетевых атак. Методы построения систем обнаружения атак.

22. Типы, возможности и способы реализации вредоносного программного кода. Классификация компьютерных вирусов по типам заражаемых областей и файлов, способам заражения, деструктивным возможностям, особенностям алгоритма.

23. Перечень уровней эшелонной защиты от вредоносного программного кода. Способы и средства реализации каждого из уровней. Назначение, возможности и практическая реализация аналитической и технической компонент защиты от вредоносного программного кода.

24. Диагностика и лечение персонального компьютера при проникновении вредоносного программного кода, в том числе компьютерных вирусов.

25. Основные интернет угрозы и правила безопасной работы в сети Интернет, в том числе безопасного поведения в социальных сетях.

Задания на умения

1. В чем заключаются отличия между односторонней, двухсторонней и трехсторонней аутентификацией?

2. В чем заключаются отличия между алгоритмическим и неалгоритмическим способами проверки PIN кода?

3. В чем заключаются отличия между системами аутентификации на основе открытого и закрытого ключа?

4. В чем заключаются отличия между аутентификацией, основанной на однонаправленных ключевых хэш-функциях и аутентификация с общим

ключом?

5. В чем заключаются отличия между криптографией и криптоанализом?

6. В чем заключаются отличия между блочным и поточным симметричным шифрованием?

7. В чем заключаются основные свойства информации с точки зрения обеспечения ее безопасности и защиты?

8. В чем заключаются отличия при определении количества ключей для симметричной и ассиметричной систем шифрования?

9. В чем заключаются отличия информационных и административных функций реализации ролевого доступа?

10. В чем заключаются отличия между избирательным и полномочным разграничением доступа?

11. В чем заключаются отличия между субъектом, объектом и методом разграничения доступа?

12. В чем заключаются отличия между функциональной и эксплуатационной безопасностью операционных систем?

13. В чем заключаются отличия между статическим и динамическим разделением обязанностей при ролевом управлении доступом?

14. В чем заключаются отличия между сегментными и персональными межсетевыми экранами?

15. В чем заключаются отличия между сегментными и встраиваемыми межсетевыми экранами?

16. В чем заключаются отличия между персональными и встраиваемыми межсетевыми экранами?

17. В чем заключаются отличия между пакетными фильтрами и Proxy серверами?

18. В чем заключаются отличия между выделенной и коммутируемой линией связи?

19. В чем заключаются отличия между VPN на основе маршрутизаторов и межсетевых экранов?

20. В чем заключаются отличия между системами обнаружения атак на уровне сети и хоста?

21. В чем заключаются отличия между средствами анализа защищенности и системами обнаружения атак?

22. В чем заключаются отличия между DDOS атакой и атакой-вторжением?

23. В чем заключаются отличия компьютерных вирусов по деструктивным возможностям?

24. В чем заключаются отличия компьютерных вирусов по особенностям алгоритма?

25. В чем заключаются отличия компьютерных вирусов по «среде обитания»?

Задания на навыки

Задание № 1.

Для представленной топологии ЛВС (технической архитектуры) определить комплекс средств идентификации и аутентификации исходя из поставленной задачи, доработать топологию ЛВС соответствующим образом.

Задание № 2.

С помощью программы Crypton:

- создать на съемном носителе Главный ключ шифрования;
- создать на жестком диске Ключ пользователя, зашифрованный на Главном ключе;
- провести зашифровывание и расшифровывание текстового файла на Ключе пользователя.

Задание № 3.

С помощью программы Crypton:

- создать на съемном носителе Главный ключ шифрования;
- создать на съемном носителе сетевую таблицу и набор из нескольких сетевых ключей;
- провести зашифровывание и расшифровывание текстового файла на определенном сетевом ключе.

Задание № 4.

Зашифровать и расшифровать сообщение с помощью шифра Вижинера.

Задание № 5.

Определить, сколько ключей необходимо для организации защищенных каналов между абонентами заданной сети, при использовании:

- симметричной системы шифрования
- асимметричной системы шифрования

и обеспечения связи «каждый с каждым».

Задание № 6.

В операционной системе Windows 7 и выше настроить политику учетных записей.

Задание № 7.

В операционной системе Windows 7 и выше настроить локальные политики (политика аудита, назначение прав пользователей, параметры безопасности)

Задание № 8.

Для представленной топологии ЛВС (технической архитектуры)

определить комплекс средств межсетевого экранирования исходя из поставленной задачи, доработать топологию ЛВС соответствующим образом.

Задание № 9.

Для представленной топологии ЛВС (технической архитектуры) определить комплекс средств организации виртуальной защищенной сети (VPN) исходя из поставленной задачи, доработать топологию ЛВС соответствующим образом.

Задание № 10.

Для представленной топологии ЛВС (технической архитектуры) определить комплекс средств защиты от сетевых атак исходя из поставленной задачи, доработать топологию ЛВС соответствующим образом.

Задание № 11.

Настроить антивирусную программу, например, 360 Total Security (эвристический анализ, уровень безопасности, алгоритмы действий с обнаруженным вредоносным программным кодом).

Задание № 12.

Провести поиск вредоносного программного кода на ПК и съемных носителях с использованием антивирусной программы, например, 360 Total Security.

Задание № 13

С помощью программы AVZ:

- провести анализ плагинов, подключенных к встроенному браузеру, выяснить, нет ли среди них подозрительных
- провести анализ приложений, разово установленных при входе в Windows нового пользователя и автоматически запускающихся при его повторных входах в Windows, выяснить, нет ли среди них подозрительных
- провести проверку системы выбрав любую папку, содержащую не менее 5 файлов, и настроив минимальные параметры эвристики
- запустить модуль слежения за запуском процессов и загрузкой драйверов, повторить проверку системы, сравнить результаты и объяснить разницу

Задание № 14

С помощью программы AVZ:

- провести поиск данных в файлах, сохраняемых браузерами при просмотре Web страниц, в качестве данных используйте условный адрес электронной почты и условные 4 цифры номера банковской карты
- провести анализ подключенных к Explorer модулей расширения

- провести проверку системы выбрав любую папку, содержащую не менее 5 файлов, и настроив минимальные параметры эвристики
- запустить модуль разграничения доступа запущенных приложений к системе, повторить проверку системы, сравнить результаты и объяснить разницу

Задание № 15

С помощью программы AVZ:

- провести расчет и сравнение контрольных сумм файлов для любой папки, содержащей не менее 5 файлов;
- провести анализ базы, содержащей данные доменных имен и используемой при их трансляции в сетевые адреса узлов, выявить, нет ли в ней несоответствий доменных имен и адресов узлов;
- провести анализ очереди задач, выяснить, нет ли среди них подозрительных
- провести поиск причины сбоев в работе программ, вызванных установкой в систему некоторых перехватчиков

Задание № 16

С помощью программы AVZ:

- провести анализ программ, запускающихся автоматически при загрузке операционной системы, выяснить, нет ли среди них подозрительных;
- провести поиск приложений по произвольному ключу, провести анализ ключей приложений, выяснить, нет ли среди них подозрительных;
- провести анализ списков поставщиков службы имен и транспорта, выяснить, нет ли среди них подозрительных;
- сохранить текущие данные о состоянии реестра, провести исследование и лечение системы, после чего восстановить сохранные данные реестра.