Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

УТВЕРЖДАЮ
Проректор по
образовательной деятельности
__________________ А.А.Панфилов
«_26_» _____08_____ 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА СОХРАННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И РЕСУРСОВ ОРГАНИЗАЦИИ

(наименование дисциплины)

Специальность подготовки	38.05.01 "Экономическая безопасность "
Специализация подготовки	«Экономико-правовое обеспечение экономической безопасности»
Уровень высшего образования	Специалитет
Форма обучения	Очная

Семестр	Трудоемкость зач. ед,/ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточной аттестации (экз./зачет)
4	4 /144	18	36		63	Экзамен (27)
Итого	4 /144	18	36		63	Экзамен (27)

Владимир 2019

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Программно-аппаратные средства сохранности информационных систем и ресурсов» - формирование у специалистов знаний и компетенций в области обеспечения сохранности информационных систем и ресурсов организации с помощью комплекса программно-аппаратных средств общего и специального назначения.

Задачи – теоретическая и практическая подготовка специалистов к деятельности, связанной с комплексным анализом возможных угроз информационным системам и ресурсам организации, знанием моделей нарушителя безопасности, постановкой конкретных задач обеспечения информационной безопасности автоматизированных систем, знанием средств и методов обеспечения сохранности информационных систем и ресурсов (ИСиР).

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Программно-аппаратные средства сохранности информационных систем и ресурсов» относится к базовой части.

Пререквизиты дисциплины: «Информатика», «Информационные технологии в профессиональной деятельности», «Информационные системы в экономике».

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код формируемых компетенций	Уровень освоения компетенции	Планируемые результаты обучения по дисциплине характеризующие этапы формирования компетенций (показатели освоения компетенции)
1	*2*	*3*
ОК-12	Частичное	**знать:** программно-аппаратные средства обеспечения информационной безопасности в операционных системах, системах управления базами данных, компьютерных сетях) **уметь:** • проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня сохранности ИС и Р; • выбирать и применять средства защиты ИСиР от вредоносного программного обеспечения; • выбирать и применять средства защиты ИСиР от несанкционированного доступа; • выбирать и применять аппаратные средства защиты ИСиР, средства криптографической защиты, биометрические средства идентификации) **владеть:** • навыками эксплуатации и администрирования в части, касающейся разграничения доступа, аутентификации и аудита баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности; • навыками использования программно-аппаратных средств обеспечения безопасности и сохранности ИС и Р (ОК-12).

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Объем уч работы с применением интерактивных методов (в час/%)	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	СРС		
1	Нормативно-правовые и технические требования к программно-аппаратным средствам сохранности информационных систем и ресурсов (ИСиР) организации	4	1-2	2	4		8	3/50	
2	Программные средства обеспечения сохранности ИСиР средствами операционных система и систем управления базами данных	4	3-6	4	8		12	6/50	1 р-к
3	Тема 3. Программно-аппаратные средства защиты ИСиР от несанкционированного доступа	4	7-10	4	8		12	6/50	
4	Тема 4. Средства защиты ИСиР от вредоносного программного обеспечения	4	11-14	3	6		9	5/55	2 р-к
5	Тема 5. Аппаратные средства защиты ИСиР, средства криптографической защиты, биометрические средства идентификации	4	15-17	3	6		10	5/55	3 р-к
6	Тема 6. Комплексные системы обеспечения сохранности ИСиР	4	18	2	4		12	3/50	
Всего за 4-й семестр				18	36		63	28/52	экзамен
Наличие в дисциплине КП/КР					–				
Итого по дисциплине				**18**	**36**		**63**	**28/52**	**экзамен**

СОДЕРЖАНИЕ ЛЕКЦИОННЫХ ЗАНЯТИЙ ДИСЦИПЛИНЫ

Тема 1.Нормативно-правовые и технические требования к программно-аппаратным средствам сохранности информационных систем и ресурсов (ИСиР) организации

Общие положения теории информационной безопасности. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий.

Определение места программно-аппаратных средств защиты информации в общей проблеме информационной безопасности. Информационные риски и статистика угроз для информации. Понятие безопасности информации и комплекс угроз в отношении оборудования пользователя и вычислительной сети.

Несанкционированный доступ (НСД). Политика безопасности организации и определение субъекта, потенциально совершающего несанкционированные действия. Статьи уголовного кодекса, предусматривающие ответственность за компьютерные преступления. Показатели защищенности средств вычислительной техники от несанкционированного доступа.

Классы защищенности автоматизированных систем. Сертификация средств защиты информации; Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно- аппаратные средства защиты информации в сетях передачи данных.

Стандарты и рекомендации в области информационной безопасности. Сущность и общее содержание комплексной системы обеспечения безопасности ЭВМ и сетей на их основе с применением программно- аппаратных средств защиты информации в информационных технологиях коммерческой организации. Задачи и методологические основы использования программно- аппаратных средств защиты информации в компьютерах. Технические требования стандартов к программно-аппаратным средствам защиты информации. Международный стандарт критериев оценки безопасности информационных технологий и ГОСТ Р ИСО/МЭК 15408-2002. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Концепция диспетчера доступа. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите. Их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем

Тема 2. Программные средства обеспечения сохранности ИСиР средствами операционных система и систем управления базами данных

Основные компоненты подсистемы защиты операционных систем. Файловая система – как основа подсистемы защиты. Права доступа к элементам файловой системы. Управление процессами. Политика безопасности. Понятие домена. Особенности установления доверительных отношений. Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности. Защита информации на машинных носителях. Защита остатков информации. Понятие межсетевых экранов. Их классификация. Основные примеры конфигурации защищенных сетей с использованием межсетевых экранов. Особенности существующих свободно-распространяемых программных реализаций межсетевых экранов. Проблемы обеспечения безопасности при удалённом доступе. Протоколы аутентификации и идентификации пользователей в компьютерных сетях. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. Защита от несанкционированного доступа. Защита от вывода. Целостность БД. Аудит. Задачи и средства администратора безопасности баз данных. Классификация моделей безопасности. Особенности применения моделей безопасности в СУБД. Дискреционные (избирательные) и мандатные (полномочные) модели безопасности. БД с многоуровневой секретностью (MLS). Основные виды и причины возникновения угроз целостности СУБД, способы противодействия. Организация взаимодействия СУБД и базовой ОС. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. Метки безопасности. Использование представлений для обеспечения конфиденциальности информации в СУБД. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.

Тема 3.Программно-аппаратные средства защиты ИСиР от несанкционированного доступа (НСД)

Применение современных средств защиты от НСД. Установка и регистрация в системе защиты. Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа. Обеспечение замкнутости программной среды. Контроль целостности. Регистрация событий. Гарантированное удаление данных. Л Обеспечение защищенного подключения автономного (не входящего в состав ЛВС) компьютера к ресурсам корпоративной сети. Программно-аппаратный комплекс шифрования трафика IP. Межсетевые защитные экраны. Руководящий документ, устанавливающий классификацию межсетевых экранов.

Тема 4. Средства защиты ИСиР от вредоносного программного обеспечения

Проблема обеспечения технологической безопасности программного обеспечения. Понятие о вредоносных программах. Классификация вредоносных программ по основным свойствам и признакам. Классификация программ по степени опасности для Л защищаемой информации и компьютерной системы. Алгоритмические и программные закладки, мотивы злоумышленных действий. Распространение компьютерных вирусов. Спам (несанкционированные электронные письма). Классификация компьютерных вирусов. Деструктивные функции вредоносных программ. Механизмы вирусного заражения. Способы выявления деструктивной активности программ. Понятие о сигнатуре вредоносного программного кода. Принцип антивирусного сканирования. Антивирусные сканеры, мониторы и сетевые фильтры. Качество антивирусной программы. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности.

Тема 5. Аппаратные средства защиты ИСиР, средства криптографической защиты, биометрические средства идентификации

Шифрование файлов и областей оперативной памяти, формирование и проверка электронной цифровой подписи в соответствии с российскими стандартами. Основные функции криптобиблиотек. Пластиковые карты – характерный пример аппаратных средств. Многоуровневые схемы управления доступом. Два типа аутентификации: статическая и динамическая. Идентификационные карты. Идентификационные карточки с магнитной полосой. Карточки с интегральной микросхемой и металлическими контактами. Микропроцессорные или интеллектуальные карточки. Бесконтактные карточки. Среда использования смарт-карт в персональных компьютерах. Аппаратный ключ или токен. Процедуры биометрического опознания. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля.

Тема 6. Комплексные системы обеспечения сохранности ИСиР

Системный подход при комплексной системе обеспечения сохранности ИсиР. Оюъект защиты. Системность и комплексность рот защите ИСиР Учет совокупной эффективности системы защиты. Макроструктурные компоненты системы защиты ИСиР. Функциональные системы. Обеспечивающие системы. Технологическая составляющая системы защиты ИСиР. Управление защитой ИСиР. Информационное обеспечение защиты ИСиР.

СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ

Тема 1. Нормативно-правовые и технические требования к программно-аппаратным средствам сохранности информационных систем и ресурсов (ИСиР) организации

Тема 2. Программные средства обеспечения сохранности ИСиР средствами операционных систем.

Тема 3. Программные средства обеспечения сохранности ИСиР средствами систем управления базами данных

Тема 4. Программно-аппаратные средства защиты ИСиР от несанкционированного доступа (НСД)

Тема 5. Средства защиты ИСиР от вредоносного программного обеспечения

Тема 6. Аппаратные средства защиты ИСиР

Тема 8. Средства криптографической защиты ИСиР

Тема 9. Изучение концепции информационной безопасности информационных систем персональных данных на примере департамента социальной защиты населения администрации Владимирской области

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В преподавании дисциплины «Математические методы и модели поддержки принятия решений» используются разнообразные образовательные технологии как традиционные, так и с применением активных и интерактивных методов обучения

Активные и интерактивные методы обучения:

1. *Интерактивная лекция (тема №1,2,3,4,5);*
2. *Групповая дискуссия (тема №1,6).*

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Текущий контроль успеваемости

Рейтинг-контроль 1

1. Понятия сохранности ИС и Р.
2. Объективная необходимость обеспечения сохранности ИС и Р.
3. Объекты администрирования.
4. Структура ИС.
5. Доменная организация ИС.
6. Серверные службы.
7. Учетные записи пользователей.
8. Служба управления конфигурациями и изменениями.
9. Идентификация конфигураций.
10. Контроль за конфигурациями.
11. Аудиты/обзоры конфигураций.
12. Служба управления безопасностью.

13. Аспекты информационной безопасности.
14. Угрозы ИС и Р.
15. Классы рисков.

Рейтинг-контроль 2

1. Программные средства обеспечения информационной безопасности.
2. Аппаратные средства обеспечения информационной безопасности.
3. Методы защиты компьютерных сетей организации.
4. Модели администрирования сети.
5. Аудит ИС.
6. Аппаратно-программные платформы администрирования.
7. Программы защиты данных и ресурсов в информационных системах госучреждений РФ.
8. Эксплуатация и сопровождение средств защиты ИС.
9. Управление и обслуживание технических средств защиты ИС.
10. Средства операционных систем, обеспечивающие сохранность информационных ресурсов.
11. Журналирование как метод защиты ИС.
12. Резервное копирование как метод защиты ИС.
13. Шифрование файлов и областей оперативной памяти
14. Формирование и проверка электронной цифровой подписи в соответствии с российскими стандартами.
15. Основные функции криптобиблиотек.
16. Пластиковые карты – характерный пример аппаратных средств.

Рейтинг-контроль 3

1. Многоуровневые схемы управления доступом.
2. Два типа аутентификации: статическая и динамическая.
3. Идентификационные карты. Идентификационные карточки с магнитной полосой. Карточки с интегральной микросхемой и металлическими контактами. Микропроцессорные или интеллектуальные карточки. Бесконтактные карточки.
4. Среда использования смарт-карт в персональных компьютерах.
5. Аппаратный ключ или токен.
6. Процедуры биометрического опознания.
7. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля.
8. Системный подход при комплексной системе обеспечения сохранности ИсиР. Объект защиты. Системность и комплексность рот защите ИСиР
9. Учет совокупной эффективности системы защиты.
10. Макроструктурные компоненты системы защиты ИСиР.
11. Функциональные системы.
12. Обеспечивающие системы.
13. Технологическая составляющая системы защиты ИСиР.
14. Управление защитой ИСиР.
15. Информационное обеспечение защиты ИСиР.

Вопросы к самостоятельной работы студентов

1. Ознакомиться с законодательством РФ в области правового обеспечения ИС:

- ознакомление с определением ИС, данном в федеральном законе ФЗ - 149 «Об информации информационных технологиях и о защите информации». Составить краткое резюме статей закона №№ 1, 2, 13, 14, 16, 17.
- ознакомление с содержанием Федерального закон N 152-ФЗ "О персональных данных". Составить краткое резюме статей закона, касающихся ИС.

2. Изучить проблему, каким образом решается вопрос об электронной подписи документов для систем электронного документооборота. Составить краткое сообщение по теме «Электронная подпись в информационной системе»
3. О каких основных аспектах следует говорить при построении систем корпоративной информационной безопасности?
4. Для чего необходимо формировать политику информационной безопасности, и из каких основных разделов она состоит?
5. В каком случае ИС считается защищенной?
6. Каким образом архитектура ИС может способствовать общей информационной безопасности и почему?
7. Из каких элементов состоит трехуровневая модель оценки защищенности ИС?
8. Изучить комплекс мер по защите ресурсов персонального компьютера, реализуемый средствами операционной системы Windows.
9. Изучить комплекс мер по защите ресурсов персонального компьютера, реализуемый средствами операционной системы Linux.
10. Каковы основные современные тенденции развития технологий и средств обеспечения сохранности ИСиР организации.
11. Составить обзор и привести классификацию устройств биометрической идентификации и аутентификации, применяемых для обеспечения сохранности ресурсов организации.

Экзаменационные вопросы

1. Нормативно-правовые и технические требования к программно-аппаратным средствам сохранности информационных систем и ресурсов (ИСиР) организации
2. Общие положения теории информационной безопасности.
3. Ключевые понятия программно-аппаратных средств защиты информации и безопасных информационных технологий.
4. Место программно-аппаратных средств защиты информации в общей проблеме информационной безопасности.
5. Информационные риски и статистика угроз для информации.
6. Понятие безопасности информации и комплекс угроз в отношении оборудования пользователя и вычислительной сети.
7. Несанкционированный доступ (НСД). Политика безопасности организации и определение субъекта, потенциально совершающего несанкционированные действия.
8. Статьи уголовного кодекса, предусматривающие ответственность за компьютерные преступления.
9. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
10. Классы защищенности автоматизированных систем. Сертификация средств защиты информации.
11. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
12. Программно- аппаратные средства защиты информации в сетях передачи данных.
13. Стандарты и рекомендации в области информационной безопасности.
14. Сущность комплексной системы обеспечения безопасности ЭВМ и сетей на их основе с применением программно- аппаратных средств защиты информации в информационных технологиях коммерческой организации.

15. Задачи и методологические основы использования программно- аппаратных средств защиты информации в компьютерах.
16. Технические требования стандартов к программно-аппаратным средствам защиты информации.
17. Международный стандарт критериев оценки безопасности информационных технологий и ГОСТ Р ИСО/МЭК 15408-2002.
18. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите.
19. Программные средства обеспечения сохранности ИСиР средствами операционных система и систем управления базами данных
20. Основные компоненты подсистемы защиты операционных систем. Файловая система – как основа подсистемы защиты. Права доступа к элементам файловой системы. Политика безопасности. Понятие домена. Особенности установления доверительных отношений.
21. Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности.
22. Защита информации на машинных носителях. Защита остатков информации. Понятие и классификация межсетевых экранов. Особенности существующих свободно-распространяемых программных реализаций межсетевых экранов.
23. Проблемы обеспечения безопасности при удалённом доступе. Протоколы аутентификации и идентификации пользователей в компьютерных сетях.
24. Угрозы безопасности БД: общие и специфичные.
25. Требования безопасности БД. Защита от несанкционированного доступа. Защита от вывода. Целостность БД. Аудит.
26. Задачи и средства администратора безопасности баз данных. Классификация моделей безопасности. Особенности применения моделей безопасности в СУБД.
27. Дискреционные (избирательные) и мандатные (полномочные) модели безопасности. БД с многоуровневой секретностью (MLS).
28. Основные виды и причины возникновения угроз целостности СУБД, способы противодействия. Организация взаимодействия СУБД и базовой ОС.
29. Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя.
30. Управление набором регистрируемых событий. Анализ регистрационной информации.
31. Программно-аппаратные средства защиты ИСиР от несанкционированного доступа (НСД)
32. Применение современных средств защиты от НСД. Установка и регистрация в системе защиты.
33. Создание учетных записей. Реализация дискреционной и мандатной моделей разграничения доступа.
34. Контроль целостности. Регистрация событий. Гарантированное удаление данных.
35. Обеспечение защищенного подключения автономного (не входящего в состав ЛВС) компьютера к ресурсам корпоративной сети.
36. Программно-аппаратный комплекс шифрования трафика IP.
37. Межсетевые защитные экраны. Руководящий документ, устанавливающий классификацию межсетевых экранов.
38. Средства защиты ИСиР от вредоносного программного обеспечения
39. Проблема обеспечения технологической безопасности программного обеспечения. Понятие о вредоносных программах. Классификация вредоносных программ по основным свойствам и признакам.
40. Классификация компьютерных вирусов. Деструктивные функции вредоносных программ. Механизмы вирусного заражения. Способы выявления деструктивной активности программ.

41. Принцип антивирусного сканирования. Антивирусные сканеры, мониторы и сетевые фильтры. Качество антивирусной программы.
42. Защита от разрушающих программных воздействий. Защита программ от изменения и контроль целостности.
43. Аппаратные средства защиты ИСиР, средства криптографической защиты, биометрические средства идентификации
44. Шифрование файлов и областей оперативной памяти, формирование и проверка электронной цифровой подписи в соответствии с российскими стандартами.
45. Основные функции криптобиблиотек.
46. Пластиковые карты как пример аппаратных средств.
47. Среда использования смарт-карт в персональных компьютерах. Аппаратный ключ или токен.
48. Процедуры биометрического опознания.
49. Устройства биометрической идентификации и аутентификации для автоматизированных систем и виды контроля.
50. Комплексные системы обеспечения сохранности ИСиР
51. Системный подход при комплексной системе обеспечения сохранности ИсиР. Объект защиты. Учет совокупной эффективности системы защиты.
52. Макроструктурные компоненты системы защиты ИСиР.
53. Функциональные системы.
54. Обеспечивающие системы.
55. Технологическая составляющая системы защиты ИСиР.
56. Управление защитой ИСиР.
57. Информационное обеспечение защиты ИСиР.

Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ	
		Количество экземпляров изданий в библиотеке ВлГУ в соответствии с ФГОС ВО	Наличие в электронной библиотеке ВлГУ
1	2	3	4
Основная литература*			
1.Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014.	2014		http://www.studentlibrary.ru/book/ISBN9785940747680.html
2.Введение в информационную безопасность [Электронный ресурс] : Учебное пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев и др.; Под ред. В.С. Горбатова. - М. : Горячая линия - Телеком, 2011.	2011		http://www.studentlibrary.ru/book/ISBN9785991201605.htm
3. Бизнес-безопасность [Электронный ресурс] / Кузнецов И.Н. - М. : Дашков и К, 2012. -	2012		http://www.studentlibrary.ru/book/ISBN9785394014383.html
4. Технические, организационные и кадровые аспекты управления информационной безопасностью [Электронный ресурс]: Учебное пособие для вузов / Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. - Вып. 4. - М. : Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью").	2013		http://www.studentlibrary.ru/book/ISBN9785991202749.html
Дополнительная литература			
1. Основы управления информационной безопасностью [Электронный ресурс]: Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Вып. 1. - М.: Горячая линия - Телеком, 2013. - (Серия "Вопросы управления информационной безопасностью").	2013		http://www.studentlibrary.ru/book/ISBN9785991202718.html
2. Комплексные (интегрированные) системы обеспечения безопасности [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 7. - М. : Горячая линия - Телеком, 2013. - (Серия "Обеспечение безопасности объектов").	2012		3. http://www.studentlibrary.ru/book/ISBN9785991202381.html

3.	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : Учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; Под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - 2-е изд., стереотип. - М. : Горячая линия - Телеком, 2012.	2012		http://www.studentlibrary.ru/book/ISBN9785991202572.html

7.2 Периодические издания

1. Информационные технологии - Ежемесячный теоретический и прикладной научно-технический журнал. Издательство «Новые технологии», Москва (имеется в электронной библиотеке ВлГУ).

7.3. Интернет-ресурсы

1. Сервер информационных технологий: www.citforum.ru
2. Учебный центр Softline: www.edu.softline.ru
3. Интернет – университет информационных технологий www.intuit.ru

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

При изучении дисциплины необходим электронный мультимедийный проектор и компьютер преподавателя, для выполнения лабораторных работ необходимы персональные компьютеры студентов.

Рабочую программу составил к.т.н., доцент Карповский В.А. ______________________________
(ФИО, подпись)

Рецензент
(представитель работодателя) ____
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ВТиСУ
Протокол № ___6_____от __26.06.19_____ года
Заведующий кафедрой В.Н. Ланцов____
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии специальности 38.05.01 «Экономическая безопасность»
Протокол № ___1_____от __26.08.19_____ года
Председатель комиссии д.э.н., профессор О.А. Доничев________________________________
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на ____________ учебный год
Протокол заседания кафедры № ______ от __________ года
Заведующий кафедрой ____________________________________

Рабочая программа одобрена на ____________ учебный год
Протокол заседания кафедры № ______ от __________ года
Заведующий кафедрой ____________________________________

Рабочая программа одобрена на ____________ учебный год
Протокол заседания кафедры № ______ от __________ года
Заведующий кафедрой ____________________________________

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на ___2020/2021____ учебный год

Протокол заседания кафедры № 1 от 02.09.20 года

Заведующий кафедрой______________________________

Рабочая программа одобрена на __2021/2022______ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой______________________________

Рабочая программа одобрена на __2022/2023__ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой______________________________