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

Институт информационных технологий и радиоэлектроники
(Наименование института)

УТВЕРЖДАЮ:
Директор института
_____ А.А. Галкин
«_26_» _августа_ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
(наименование дисциплины)

направление подготовки / специальность

10.05.04 «Информационно-аналитические системы безопасности»
(код и наименование направления подготовки (специальности)

направленность (профиль) подготовки

Автоматизация информационно-аналитической деятельности
(направленность (профиль) подготовки))

г. Владимир

2021

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Программно-аппаратные средства защиты информации» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО 3++ и учебного плана по специальности 10.05.04 «Информационно-аналитические системы безопасности». В процессе подготовки обеспечивается формирование у студентов профессиональных навыков по эксплуатации и обслуживанию аппаратуры, оборудования и программного обеспечения, связанных с: обеспечением безопасности данных; шифрованием и защитой от несанкционированного доступа; профессиональных навыков выявления и уничтожения компьютерных вирусов; противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; навыков работы со специальной технической литературой.

Задачей дисциплины «Программно-аппаратные средства защиты информации» является создание у студентов представления о принципах, методах и средствах выявления угроз безопасности автоматизированных систем, а также развитие способностей к логическому и алгоритмическому мышлению и осуществлению проверки защищенности объектов на соответствие требованиям нормативных документов. Задачей дисциплины также является овладение навыками практической деятельности в области моделирования и анализа технических средств аппаратной и программной защиты автоматизированных систем с использованием средств вычислительной техники, умение использовать соответствующее специализированное программное обеспечение.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Программно-аппаратные средства защиты информации» относится к обязательной части Блока Б1 (код Б1.О.22). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, и лабораторных работ. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции *(код, содержание индикатора)*	Результаты обучения по дисциплине	
ОПК-11 Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации	ОПК-1.1.1	Знать программные и программно-аппаратные средства защиты информации	Тестовые вопросы
	ОПК-1.1.2	Знать методы настройки, обслуживания и восстановления средств защиты информации на всех этапах жизненного цикла ИАС	
	ОПК-1.2.1	Уметь применять защищенные протоколы, межсетевые экраны, средства обнаружения вторжений в компьютерные сети	
	ОПК-1.2.2	Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием программных и программно-аппаратных средств защиты информации	
	ОПК-1.3.1	Владеть навыками настройки, эксплуатации, обслуживания средств защиты информации на всех этапах жизненного цикла ИАС	

ОПК-13 Способен производить настройку и обслуживание компонентов обеспечивающей части информационно-аналитических систем на всех этапах жизненного цикла, встроенных средств защиты информации, восстанавливать их работоспособность при внештатных ситуациях	ОПК-13.1.1	Знать программные и программно-аппаратные средства защиты информации	Тестовые вопросы
	ОПК-13.1.2	Знать методы настройки, обслуживания и восстановления средств защиты информации на всех этапах жизненного цикла ИАС	
	ОПК-13.2.1	Уметь настраивать и обслуживать средств защиты информации на всех этапах жизненного цикла ИАС	
	ОПК-13.2.2	Уметь восстанавливать средства защиты информации ИАС в полном объеме	
	ОПК-13.2.3	Уметь использовать средства защиты, предоставляемые системами управления базами данных	
	ОПК-13.3.1	Владеть навыками восстановления работоспособности средств защиты информации ИАС при внештатных ситуациях	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	Введение (предмет и задачи программно-аппаратной защиты информации, методы и средства защиты информации)	7	1	2	2			2	
2	Уязвимость компьютерных систем.	7	2	2	2	4		2	
3	Идентификация и аутентификация	7	3	2	2			2	
4	Система разграничения доступа к информации	7	4	2	2	4		2	
5	Протоколы идентификации/аутентификации	7	5	2	2			2	
6	Методы и средства защиты программ от компьютерных вирусов	7	6	2	2	4		2	Рейтинг-контроль №1
7	Характеристика средств нейтрализации компьютерных вирусов.	7	7	2	2			2	

8	Оценка антивирусов	7	8	2	2	4		2	
9	Общая характеристика программно-аппаратных средств защиты информации	7	9	2	2			2	
10	Общая характеристика электронных идентификаторов	7	10	2	2	4		2	
11	Защита программ от программных закладок.	7	11	2	2			2	
12	Методы и способы защиты программ от исследования.	7	12	2	2	4		2	Рейтинг-контроль №2
13	Защита программ от несанкционированного копирования.	7	13	2	2			2	
14	Системы обнаружения атак и вторжений.	7	14	2	2	4		2	
15	Электронная цифровая подпись (ЭЦП)	7	15	2	2			2	
16	**Раздел 16.** Архитектура ПАСЗИ (конфигурации средств защиты; методы реализации; функционал и особенности использования).	7	16	2	2	4		2	
17	**Раздел 17.** Кейло́ггеры и другие аппаратные закладки	7	17	2	2			2	
18	**Раздел 18.** Нормативная база государственных регуляторов России и действующие стандарты в области использования ПАСЗИ	7	18	2	2	4		2	Рейтинг-контроль №3
Всего за 7 семестр:		**144**		**36**	**36**	**36**		**36**	**Зачет с оценкой**
Итого по дисциплине		**144**		**36**	**36**	**36**		**36**	**Зачет с оценкой**

Содержание лекционных занятий по дисциплине

Раздел 1. Введение (предмет и задачи программно-аппаратной защиты информации; методы и средства защиты информации и предотвращения несанкционированного доступа). Основные понятия.

Раздел 2. Уязвимость компьютерных систем. Политика безопасности в компьютерных системах. Оценка защищенности. Абстрактные модели защиты информации Модель Биба; Модель Гогена–Мезигера ; Сазерлендская модель; Модель Кларка-Вильсона.

Раздел 3. Идентификация и аутентификация (идентификация пользователей (субъектов доступа к данным). Процедура идентификации и аутентификации. Однофакторная и двухфакторная идентификации. Биометрические методы идентификации и аутентификации. Технологии автоматической идентификации.

Раздел 4. Система разграничения доступа к информации (архитектура системы; концепция построения систем разграничения доступа; модели разграничения доступа; надежность систем разграничения доступа).

Раздел 5. Протоколы идентификации/аутентификации (обобщенный алгоритм, на основе алгоритма RSA, схемы Фейге-Фиата-Шамира, Эль-Гамаля, Шнорра). Протоколы идентификации с нулевой передачей знаний. Протоколы Kerberos, S/Key (RFC 1760), PAP и CHAP, OpenID, Windows Live ID, LDAP, OpenLDAP.

Раздел 6. Методы и средства защиты программ от компьютерных вирусов (характеристика и классификация компьютерных вирусов.

Раздел 7. Характеристика средств нейтрализации компьютерных вирусов. Технологии обнаружения вирусов, антивирусные комплексы.
Раздел 8. Оценка антивирусов; требования к средствам антивирусной защиты ФСТЭК России. Классификация методов защиты от компьютерных вирусов.
Раздел 9. Общая характеристика программно-аппаратных средств защиты информации (классификация средств защиты; государственный реестр сертифицированных средств защиты информации; краткая характеристика средства защиты СЗИ Secret Net, ПАК Криптон, Honeypot Manager, КИБ SearchInform, Secret Disk и т.д.)
Раздел 10. Общая характеристика электронных идентификаторов (идентификаторы eToken, JaCarta, Maxim (iButton), Sentinel, Guardant, Rutoken, CmDongle, WibuKey, SenseLock, LOCK и т.д.).
Раздел 11. Защита программ от программных закладок. Способы внедрения закладок. Классификация недекларированных возможностей программного обеспечения. Методы вскрытия недекларированных возможностей. Подходы выявления дефектов в программном обеспечении, возможные методы защиты.
Раздел 12. Методы и способы защиты программ от исследования. Классификация средств исследования программ. Методы защиты программ от исследования.
Раздел 13. Защита программ от несанкционированного копирования. Методы, затрудняющие считывание скопированной информации. Методы, препятствующие использованию скопированной информации. Основные функции средств защиты от копирования. Основные методы защиты от копирования. Методы противодействия динамическим способам снятия защиты программ от копирования.
Раздел 14. Системы обнаружения атак и системы обнаружения вторжений. Классификация. Методы обнаружения сигнатур и методы обнаружения аномалий.
Раздел 15. Электронная цифровая подпись (ЭЦП). Понятие ЭЦП, основные алгоритмы реализации ЭЦП.
Раздел 16. Архитектура ПАСЗИ (конфигурации средств защиты; методы реализации; функционал и особенности использования).
Раздел 17. Кейло́ггеры и другие аппаратные закладки на основе микропроцессоров и микроконтроллеров, классификация, возможности и методы противодействия. Программно-аппаратные закладки для мобильных сетей. Программно-аппаратные средства защиты мобильных сетей.
Раздел 18. Нормативная база государственных регуляторов России и действующие стандарты в области использования ПАСЗИ.

Содержание лабораторных занятий по дисциплине

Лабораторные работы:
Лабораторная работа 1. Разработка ПО разграничения полномочий пользователей
Лабораторная работа 2. Защита программного обеспечения от изменения и копирования.
Лабораторная работа 3. Разработка и программная реализация криптографических алгоритмов.
Лабораторная работа 4. Изучение способов формирования электронной цифровой подписи (ЭЦП) на основе КриптоПро CSP 3.9 R2 / КриптоПро CSP 4.0 - для Windows 10
Лабораторная работа 5. Изучение способов формирования электронной цифровой подписи (ЭЦП) на основе ViPNet CSP 4.2 - для Windows 10
Лабораторная работа 6. Организация защищенного обмена информацией на основе использования программы PGP
Лабораторная работа 7. Организация защищенного канала с помощью VPN
Лабораторная работа 8. Программная реализация защиты программ с помощью электронных ключей типа «HASP HL Pro»

Содержание практических занятий по дисциплине

Практическое занятие 1. Принципы защиты программ от копирования с помощью электронных ключей. Пристыковочный механизм и механизм использования API.

Практическое занятие 2. Особенности реализации асимметричных систем шифрования, защита файлов от изменения с помощью электронной цифровой подписи, имитовставки. Контроль целостности сообщений путем шифрования, использования хэш-функций, кодов аутентификации сообщений.

Практическое занятие 3. Защита от отладки, защита от дизассемблирования, защита от трассировки по прерываниям, защита программ от изменения и разрушающего воздействия.

Практические занятия 4-5. Общий сравнительный обзор современных программно-аппаратных средств защиты информации (назначение, технические характеристики, особенности установки и эксплуатации, демоверсии ПО) CSP VPN Gate; CSP VPN Server; Honeypot Manager; ViPNet BOX; ViPNet CUSTOM; АПКШ Континент; ИВК Кольчуга; Комплекс DeviceLock; Комплекс Diamond VPN/FW; Комплекс Ideco ICS 3; Комплекс InfoWatch Traffic Monitor; Контур ИБ SearchInform; ПАК SafeNet; ПАК Аргус; ПАК Лабиринт-ДЗ; ПАК Панцирь; ПАК Соболь; ПАК Росомаха; ПАК Криптон; ПАК ФПСУ-IP; Па-кет программ "ЗАСТАВА"; ПКЗИ Dallas Lock; ПО TERRIER; ПО Ревизор-1 (Ревизор-2); ПО Трафа-рет; ПО Тритон; ПО ФИКС; Сервер DioNIS; СЗИ Crypton Lock; СЗИ Diamond ACS; СЗИ Secret Disk; СЗИ Secret Net; СЗИ TrustAccess; СЗИ vGate; СЗИ Аура; СЗИ Блокпост-2000/XP; СЗИ Блокхост-сеть; СЗИ Шипка; СЗИ Эгида+; Система КУБ; Система Форпост; СКЗ MaxPatrol; Устройство Proventia Network IPS и др.

Практические занятия 6-7. Общий сравнительный обзор современных систем обнаружения вторжений (назначение, технические характеристики, особенности установки и эксплуатации, демоверсии ПО) Cisco IPS/IDS, McAfee Network Security Platform, Stonesoft StoneGate IPS, АПКШ «Континент», ViPNet IDS, Check Point IPS, Snort, Рубикон, MaxPatrol SIEM и др.

Практическое занятие 8. Общий сравнительный обзор современных кейло́ггеров, аппаратных закладок на основе микропроцессоров и микроконтроллеров (назначение, технические характеристики, особенности установки и эксплуатации, демоверсии ПО).

Практическое занятие 9. Общий сравнительный обзор современных аппаратных закладок для мобильных сетей (назначение, технические характеристики, особенности установки и эксплуатации, демоверсии ПО).

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

5.1. Текущий контроль успеваемости

Перечень вопросов к рейтинг-контролю №1

- Основные задачи программно-аппаратной защиты информации
- Основные методы и средства защиты информации с помощью ПАСЗИ
- Основные методы предотвращения несанкционированного доступа
- Политика безопасности в компьютерных системах
- Уязвимость компьютерных систем. Оценка защищенности в компьютерных системах
- Абстрактные модели защиты информации Модель Биба; Модель Гогена–Мезигера; Сазерлендская модель; Модель Кларка-Вильсона
- Идентификация пользователей (субъектов доступа к данным).
- Биометрические методы идентификации и аутентификации.
- Технологии автоматической идентификации
- Протоколы идентификации/аутентификации (обобщенный алгоритм).
- Протоколы идентификации/аутентификации (на основе алгоритма RSA).

- Протоколы идентификации/аутентификации (схема Фейге-Фиата-Шамира).
- Протоколы идентификации/аутентификации (схема Эль-Гамаля).
- Протоколы идентификации/аутентификации (схема Шнорра).
- Протоколы идентификации с нулевой передачей знаний.

Перечень вопросов к рейтинг-контролю №2

- Протокол Kerberos.
- Протоколы S/Key (RFC 1760), PAP и CHAP.
- Протоколы OpenID, Windows Live ID.
- Протоколы LDAP, OpenLDAP.
- Единая система идентификации и аутентификации РФ.
- Система разграничения доступа к информации.
- Методы защиты программ от компьютерных вирусов
- Средства защиты программ от компьютерных вирусов
- Характеристика и классификация компьютерных вирусов
- Характеристика средств нейтрализации компьютерных вирусов. Технологии обнаружения вирусов, антивирусные комплексы.
- Оценка антивирусов; требования к средствам антивирусной защиты ФСТЭК России. Классификация методов защиты от компьютерных вирусов
- Общая характеристика программно-аппаратных средств защиты информации (классификация средств защиты; государственный реестр сертифицированных средств защиты информации)
- Общая характеристика электронных идентификаторов (классификация, назначение, характеристики)
- Защита программ от программных закладок. Способы внедрения закладок.
- Классификация недекларированных возможностей программного обеспечения.
- Методы вскрытия недекларированных возможностей программного обеспечения.

Перечень вопросов к рейтинг-контролю №3

- Подходы выявления дефектов в программном обеспечении, возможные методы защиты.
- Классификация средств исследования программ
- Методы защиты программ от исследования.
- Методы, затрудняющие считывание скопированной информации.
- Методы, препятствующие использованию скопированной информации.
- Основные функции средств защиты от копирования.
- Методы противодействия динамическим способам снятия защиты программ от копирования.
- Системы обнаружения атак и системы обнаружения вторжений. Классификация.
- Методы обнаружения сигнатур в системах обнаружения вторжений
- Методы обнаружения аномалий в системах обнаружения вторжений
- Понятие ЭЦП, виды ЭП, основные алгоритмы реализации ЭЦП
- Понятие удостоверяющих центров (УЦ), требования к УЦ
- Кейло́ггеры и другие аппаратные закладки на основе микропроцессоров и микроконтроллеров, классификация, возможности и методы противодействия
- Программно-аппаратные закладки для мобильных сетей
- Программно-аппаратные средства защиты мобильных сетей
- Требования международных стандартов в области использования ПАСЗИ
- Нормативная база государственных регуляторов России по применению ПАСЗИ для защиты АИС

5.2. Промежуточная аттестация

Примерный перечень вопросов к зачету с оценкой

1. Основные задачи программно-аппаратной защиты информации
2. Основные методы и средства защиты информации с помощью ПАСЗИ
3. Основные методы предотвращения несанкционированного доступа
4. Политика безопасности в компьютерных системах
5. Уязвимость компьютерных систем. Оценка защищенности в компьютерных системах
6. Абстрактные модели защиты информации Модель Биба; Модель Гогена–Мезигера; Сазерлендская модель; Модель Кларка-Вильсона
7. Идентификация пользователей (субъектов доступа к данным).
8. Биометрические методы идентификации и аутентификации.
9. Технологии автоматической идентификации
10. Протоколы идентификации/аутентификации (обобщенный алгоритм).
11. Протоколы идентификации/аутентификации (на основе алгоритма RSA).
12. Протоколы идентификации/аутентификации (схема Фейге-Фиата-Шамира).
13. Протоколы идентификации/аутентификации (схема Эль-Гамаля).
14. Протоколы идентификации/аутентификации (схема Шнорра).
15. Протоколы идентификации с нулевой передачей знаний.
16. Протокол Kerberos.
17. Протоколы S/Key (RFC 1760), PAP и CHAP.
18. Протоколы OpenID, Windows Live ID.
19. Протоколы LDAP, OpenLDAP.
20. Единая система идентификации и аутентификации РФ.
21. Система разграничения доступа к информации.
22. Методы защиты программ от компьютерных вирусов
23. Средства защиты программ от компьютерных вирусов
24. Характеристика и классификация компьютерных вирусов
25. Характеристика средств нейтрализации компьютерных вирусов. Технологии обнаружения вирусов, антивирусные комплексы.
26. Оценка антивирусов; требования к средствам антивирусной защиты ФСТЭК России. Классификация методов защиты от компьютерных вирусов
27. Общая характеристика программно-аппаратных средств защиты информации (классификация средств защиты; государственный реестр сертифицированных средств защиты информации)
28. Общая характеристика электронных идентификаторов (классификация, назначение, характеристики)
29. Защита программ от программных закладок. Способы внедрения закладок.
30. Классификация недекларированных возможностей программного обеспечения.
31. Методы вскрытия недекларированных возможностей программного обеспечения.
32. Подходы выявления дефектов в программном обеспечении, возможные методы защиты.
33. Классификация средств исследования программ
34. Методы защиты программ от исследования.
35. Методы, затрудняющие считывание скопированной информации.
36. Методы, препятствующие использованию скопированной информации.
37. Основные функции средств защиты от копирования.
38. Методы противодействия динамическим способам снятия защиты программ от копирования.
39. Системы обнаружения атак и системы обнаружения вторжений. Классификация.
40. Методы обнаружения сигнатур в системах обнаружения вторжений
41. Методы обнаружения аномалий в системах обнаружения вторжений
42. Понятие ЭЦП, виды ЭП, основные алгоритмы реализации ЭЦП
43. Понятие удостоверяющих центров (УЦ), требования к УЦ

44. Кейло́ггеры и другие аппаратные закладки на основе микропроцессоров и микроконтроллеров, классификация, возможности и методы противодействия
45. Программно-аппаратные закладки для мобильных сетей
46. Программно-аппаратные средства защиты мобильных сетей
47. Требования международных стандартов в области использования ПАСЗИ
48. Нормативная база государственных регуляторов России по применению ПАСЗИ для защиты АИС

5.3. Самостоятельная работа обучающегося.

Примерные вопросы и задания для самостоятельной работы студентов

- Идентификация пользователей (субъектов доступа к данным). Биометрические признаки, которые могут быть использованы при идентификации.
- Технологий автоматической идентификации. Штриховые коды (символики). Радиочастотная идентификация.
- Система разграничения доступа к информации. Функциональные блоки. Концепция построения.
- Механизмы управления доступом (модели разграничения доступа). Дискреционное управление доступом.
- Механизмы управления доступом (модели разграничения доступа). Мандатное управление доступом.
- Механизмы управления доступом (модели разграничения доступа). Управление доступом на основе ролей.
- Надежность систем разграничения доступа. Интенсивность отказов. Среднее время восстановления системы защиты после отказа.
- Методы предотвращения утечек из КС. Классификация внутренних ИТ-угроз.
- Методы предотвращения утечек из КС. Законный перехват данных.
- Методы предотвращения утечек из КС. Обобщенный процесс выбора систем DLP.
- Методы и средства защиты программ от компьютерных вирусов. Общая характеристика и классификация.
- Методы и средства защиты программ от компьютерных вирусов. Общая характеристика средств нейтрализации компьютерных вирусов. Методы защиты от компьютерных вирусов.
- Методы защиты программ от исследования. Сфера применения. Компоненты системы защиты и их функции.
- Способы защиты программ от исследования. 4-е класса способов защиты

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература*		
Программно-аппаратные средства защиты информационных систем: учебное пособие : [16+] / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. ISBN 978-5-8265-1737-6.	2017	https://biblioclub.ru/index.php?page=book&id=499013 (дата обращения: 25.08.2021)

Технологии обеспечения безопасности информационных систем : учебное пособие: [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с ISBN 978-5-4499-1671-6. – DOI 10.23681/598988	2021	https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 25.08.2021)
Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем: курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу / А. М. Голиков. – Томск: ТУСУР, 2016. – 396с	2016	https://biblioclub.ru/index.php?page=book&id=480796 (дата обращения: 25.08.2021)
Технологии защиты информации в компьютерных сетях / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с.	2016	https://biblioclub.ru/index.php?page=book&id=428820 (дата обращения: 25.08.2021)
Долозов, Н. Л. Программные средства защиты информации: конспект лекций / Н. Л. Долозов, Т. А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2015. – 63 с. ISBN 978-5-7782-2753-8	2015	https://biblioclub.ru/index.php?page=book&id=438307 (дата обращения: 25.08.2021)
Дополнительная литература		
Белоус, А. И. Основы кибербезопасности: стандарты, концепции, методы и средства обеспечения : [16+] / А. И. Белоус, В. А. Солодуха. – Москва : Техносфера, 2021. – 482 с. ISBN 978-5-94836-612-8.	2021	https://biblioclub.ru/index.php?page=book&id=617523 (дата обращения: 25.08.2021)
Белоус, А. И. Программные и аппаратные трояны — способы внедрения и методы противодействия: первая техническая энциклопедия : в 2 книгах / А. И. Белоус, В. А. Солодуха, С. В. Шведов. – Москва: Техносфера, 2019. – Книга 1. – 1318 с. ISBN 978-5-94836-524-4	2019	https://biblioclub.ru/index.php?page=book&id=597000 (дата обращения: 25.08.2021)
Мэйволд, Э. Безопасность сетей : учебное пособие : [16+] / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с.	2016	https://biblioclub.ru/index.php?page=book&id=429035 (дата обращения: 25.08.2021)
Басыня, Е. А. Системное администрирование и информационная безопасность: учебное пособие: [16+] / Е. А. Басыня. – Новосибирск: Новосибирский государственный технический университет, 2018. 79с. ISBN 978-5-7782-3484-0. – Текст : электронный.	2018	https://biblioclub.ru/index.php?page=book&id=575325 (дата обращения: 25.08.2021)

6.2. Периодические издания

1. Электронный журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: http://inside-zi.ru/pages/about.html
2. Электронный журнал «Спецтехника и Связь», Режим доступа: http://www.st-s.su/
3. Электронный журнал «Системы безопасности связи и телекоммуникаций» –компания «Гротек», Москва [Электронный ресурс] // URL: http://sccs.intelgr.com/
4. Электронный научно-технический журнал «Специальная техника», Москва [Электронный ресурс] // URL: http://www.ess.ru/
5. Электронный журнал «БДИ» (Безопасность, Достоверность, Информация), С.-Петербург. [Электронный ресурс] // URL: http://asbgroup.ru/izdaniya/zhurnal-bdi/

6.3. Интернет-ресурсы

1. Сайт ФСТЭК России [Электронный ресурс] // URL: https://fstec.ru/
2. Сайт «Группа СТ» г. Санкт-Петербург [Электронный ресурс] // URL: http://spymarket.com/
3. Сайт «Группа компаний «Маском»» г.Москва [Электронный ресурс] // URL: http://www.mascom.ru/ (дата обращения: 13.06.2018).

4. Сайт ЗАО НПЦ Фирма "НЕЛК" г. Москва [Электронный ресурс] // URL: https://www.nelk.ru/
5. Сайт «НПО Защита информации» г. Москва [Электронный ресурс] // URL: http://www.sinf.ru/
6. Сайт компании «Проминформзащита» г. Москва [Электронный ресурс] // URL: http://www.profinfo.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил _____ доцент кафедры ИЗИ Тельный А.В.
(ФИО, должность, подпись)

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр» к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 26.08.21 года
Заведующий кафедрой д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена
на заседании учебно-методической комиссии специальности 10.05.04 «Информационно-аналитические системы безопасности»

Протокол № 1 от 26.08.21 года
Председатель комиссии д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, должность, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20 22 / 20 23 учебный год

Протокол заседания кафедры № 14 от 28.06.22 года

Заведующий кафедрой д.т.н., профессор _____ /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор _____ /М.Ю. Монахов/

Рабочая программа одобрена на 20____ / 20____ учебный года

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор _____ /М.Ю. Монахов/

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

Программно-аппаратные средства защиты информации

образовательной программы специальности

10.05.04 «Информационно-аналитические системы безопасности»

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой д.т.н., профессор _____/М.Ю. Монахов/_

Подпись *ФИО*