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

УТВЕРЖДАЮ:
Директор института
_____Галкин А.А
«_06_» _07_____2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ
(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

2022 год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Безопасность информационных и аналитических систем» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО и учебного плана по специальности 10.05.04 «Информационно-аналитические системы безопасности», ознакомление студентов с технологиями безопасного с точки зрения возможности утечки информации интеллектуального анализа больших информационных массивов посредством и с помощью информационно-аналитических систем.

Основными задачами изучения курса является**:** изучение основных положений, понятий и категорий, связанных с обеспечением безопасности информационно-аналитических систем; изучение основных подходов к выполнению безопасного интеллектуального анализа больших массивов данных посредством современных информационных технологий; формирование навыков противодействия несанкционированному проникновению в защищаемые информационные и аналитические системы с использованием современных информационно-вычислительных средств и систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Безопасность информационно аналитических систем» относится к обязательной части образовательной программы, код Б1.О.03 специальности 10.05.04 «Информационно-аналитические системы безопасности». В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и самостоятельной работы студентов. 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-6 Способен при решении профессиональных задач проверять выполнение требований защиты информации ограниченного доступа в информационно-аналитических системах в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.1.1	Знать основные отечественные и зарубежные стандарты в области компьютерной безопасности	Тестовые вопросы
	ОПК-6.1.2	Знать основные методы организационного обеспечения информационной безопасности специальных информационно-аналитических систем	
	ОПК-6.1.3	Знать механизмы реализации атак в компьютерных сетях	
	ОПК-6.1.4	Знать защитные механизмы и средства обеспечения сетевой безопасности	
	ОПК-6.2.1	Уметь умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях	

	ОПК-6.2.2	Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты информации	
	ОПК-6.2.3	Уметь пользоваться средствами защиты, предоставляемыми системами управления базами данных	
	ОПК-6.2.4	Уметь применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем	
	ОПК-6.2.5	Уметь применять средства антивирусной защиты и обнаружения вторжений в компьютерные сети	
	ОПК-6.2.6	Уметь разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками	
	ОПК-6.3.1	Владеть навыками настройки межсетевых экранов	
	ОПК-6.3.2	Владеть методикой анализа сетевого трафика	
	ОПК-6.3.3	Владеть методикой анализа результатов работы средств обнаружения вторжений в компьютерные сети	
	ОПК-6.3.4	Владеть методами и средствами выявления угроз безопасности компьютерным системам	
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 нормативные правовые акты в области защиты информации	Тестовые вопросы
	ОПК-13.1.2	Знать руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	
	ОПК-13.1.3	Знать организационные меры по защите информации	
	ОПК-13.1.4	Знать методы настройки, обслуживания и восстановления средств защиты информации на всех этапах жизненного цикла информационно-аналитических систем	
	ОПК-13.1.5	Знать механизмы реализации атак в компьютерных сетях	
	ОПК-13.1.6	Знать защитные механизмы и средства обеспечения сетевой безопасности	
	ОПК-13.2.1	Уметь умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях	
	ОПК-13.2.2	Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных	

		средств защиты информации	
	ОПК-13.2.3	Уметь пользоваться средствами защиты, предоставляемыми системами управления базами данных	
	ОПК-13.2.4	Уметь применять средства антивирусной защиты и обнаружения вторжений в компьютерные сети	
	ОПК-13.2.5	Уметь разрабатывать частные политики безопасности компьютерных систем, в том числе, политики управления доступом и информационными потоками	
	ОПК-13.3.1	Владеть навыками настройки межсетевых экранов	
	ОПК-13.3.2	Владеть методикой анализа сетевого трафика	
	ОПК-13.3.3	Владеть методикой анализа результатов работы средств обнаружения вторжений в компьютерные сети	
	ОПК-13.3.4	Владеть методами и средствами выявления угроз безопасности компьютерным системам	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов

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	Архитектура современных информационных и аналитических систем.	10	1-2	4		4		4	
2	Уязвимости и угрозы	10	3-4	4		4		4	
3	Протоколы идентификации учета	10	5-6	4		4		4	Рейтинг-контроль №1
4	Протоколы аутентификации учета	10	7-8	4		4		4	
5	Протоколы идентификации современных информационных и аналитических системах.	10	9-10	4		4		4	
6	Протоколы аутентификации современных информационных и аналитических системах	10	11-12	4		4		4	Рейтинг-контроль №2

7	Управление доступом в хранилищах данных	10	13-14	4		4		4	
8	Управление доступом в аналитических системах	10	15-16	4		4		4	
9	Межсетевое взаимодействие	10	17-18	4		4		4	Рейтинг-контроль №3
Всего за семестр А:		**108**		**36**		**36**		**36**	**Зачет**
1	Организация безопасного межсетевого взаимодействия	11	1-2	4		4		1	
2	Защита удаленного доступа в АИС.	11	3-4	4		4		1	
3	Защищенный удаленный доступ	11	5-6	4		4		1	Рейтинг-контроль №1
4	Организация защищенного удаленного доступа в информационных и аналитических системах.	11	7-8	4		4		1	
5	Управление криптоключами	11	9-10	4		4		1	
6	Управление криптоключами в информационных и аналитических системах	11	11-12	4		4		1	Рейтинг-контроль №2
7	Инфраструктура управления открытыми ключами PKI	11	13-14	4		4		1	
8	Стандарт Public-Key	11	15-16	4		4		1	
9	Стандарт Cryptography	11	17-18	4		4		1	Рейтинг-контроль №3
Всего за семестр В		**108**		**36**		**36**		**9**	**Экзамен(27)**
Наличие в дисциплине КП/КР		**Нет**							
Итого по дисциплине		**216**		**72**		**72**		**45**	**Зачет Экзамен(27)**

Содержание лекционных занятий по дисциплине

Семестр А

Тема 1. Архитектура современных информационных и аналитических систем.

Тема 2. Уязвимости и угрозы современных информационных и аналитических систем. Методы обеспечения ИБ информационных и аналитических систем

Тема 3. Протоколы идентификации и учета в современных информационных и аналитических системах.

Тема 4. Протоколы аутентификации в современных информационных и аналитических системах. Методы локальной аутентификации

Тема 5. Протоколы идентификации и аутентификации современных информационных и аналитических системах. Протокол TACACS.

Тема 6. Протоколы идентификации и аутентификации современных информационных и аналитических системах Протокол RADIUS.

Тема 7. Управление доступом в хранилищах данных информационных и аналитических систем.

Тема 8. Управление доступом в аналитических системах. Иерархия прав доступа. Виды привилегий.

Тема 9. Межсетевое взаимодействие

Семестр В

Тема 1. Организация безопасного межсетевого взаимодействия в распределенных информационных и аналитических системах. Организация безопасного межсетевого взаимодействия в распределенных информационных и аналитических системах. IPSec

Тема 2. Защита удаленного доступа в АИС

Тема 3. Организация защищенного удаленного доступа в информационных и аналитических системах

Тема 4. Протоколы защищенного удаленного доступа

Тема 5. Организация безопасного межсетевого взаимодействия

Тема 6. Защита удаленного доступа в АИС. Организация защищенного удаленного доступа в информационных и аналитических системах

Тема 7. Управление криптоключами в информационных и аналитических системах

Тема 8. Инфраструктура управления открытыми ключами PKI

Тема 9. Стандарты Public-Key Cryptography

Содержание лабораторных занятий по дисциплине

Семестр А

Лабораторная работа №1. Управление правами доступа

Лабораторная работа №2. Установка и конфигурирование сервера RADIUS

Лабораторная работа №3. Обеспечение защищенного административного доступа;

Лабораторная работа №4. Обеспечение защищенного административного доступа с применением AAA и RADIUS.

Лабораторная работа №5. Команды и алгоритм конфигурирования Site-to-Site VPN на устройствах Cisco

Лабораторная работа №6. Команды и алгоритм конфигурирования Remote-Access VPN на устройствах Cisco

Семестр В

Лабораторная работа №1. Практика конфигурирования AAA на маршрутизаторах Cisco;

Лабораторная работа №2. Практика конфигурирования site-to-site VPN;

Лабораторная работа №3. Практика конфигурирования защищенного доступа к удаленной ИАС

Лабораторная работа №4. Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Remote-Access VPN

Лабораторная работа №5. Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Site-to-Site VPN

Лабораторная работа №6. Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол IPSec.

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

Семестр А

Вопросы рейтинг-контроля №1

- Современные уязвимости программного обеспечения информационных и аналитических систем;
- Вредоносное программное обеспечение и программные средства сетевых атак
- Методы и средства защиты информационных и аналитических систем;

- Задачи, решаемые современными средствами идентификации и аутентификации в информационных и аналитических системах;
- Характеристики AAA.
- Конфигурирование локальной AAA аутентификации с CLI на устройствах Cisco

Вопросы рейтинг-контроля №2

- Управление доступом в хранилищах данных информационных и аналитических систем.
- Иерархия прав доступа. Создание ролей.
- Виды привилегий. Операторы представления привилегий.
- Управление паролями в хранилищах данных информационных и аналитических систем. Операторы отмены привилегий
- Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.

Вопросы рейтинг-контроля №3

- Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол AH. Особенности применения
- Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол ESP. Особенности применения
- Команды и алгоритм конфигурирования Site-to-Site VPN на устройствах Cisco
- Команды и алгоритм конфигурирования Remote-Access VPN на устройствах Cisco
- Политики ISAKMP. Конфигурирование Pre-Shared Key

Семестр B

Вопросы рейтинг-контроля №1

- Конфигурирование распределенной AAA аутентификации с CLI на устройствах Cisco
- Протокол TACACS+. Задачи и характеристики протокола
- Протокол RADIUS. Задачи и характеристики протокола
- Аутентификация средствами протокола TACACS+. Конфигурирование протокола на устройствах Cisco
- Аутентификация средствами протокола RADIUS. Конфигурирование протокола на устройствах Cisco
- Аутентификация с 802.1X

Вопросы рейтинг-контроля №2

- Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.
- Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Remote-Access VPN
- Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Site-to-Site VPN
- Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол IPSec.
- Протокол IPSec. Обеспечение конфиденциальности в информационных и аналитических системах.
- Протокол IPSec. Обеспечение целостности в информационных и аналитических системах.

Вопросы рейтинг-контроля №3

- Протоколы защищенного удаленного доступа в информационных и аналитических системах.
- Конфигурирование протоколов защищенного удаленного доступа в информационных и аналитических системах.

- Инфраструктура PKI. Задачи PKI
- Особенности применения ЭП в информационных и аналитических системах.
- Криптографические стандарты PKI
- Топологии PKI

5.2. Промежуточная аттестация по итогам освоения дисциплины

Примерный перечень вопросов к зачету. Семестр А

1. Современные угрозы информационной безопасности информационных и аналитических систем;
2. Современные уязвимости программного обеспечения информационных и аналитических систем;
3. Вредоносное программное обеспечение и программные средства сетевых атак
4. Методы и средства защиты информационных и аналитических систем;
5. Задачи, решаемые современными средствами идентификации и аутентификации в информационных и аналитических системах;
6. Характеристики AAA.
7. Конфигурирование локальной AAA аутентификации с CLI на устройствах Cisco
8. Конфигурирование распределенной AAA аутентификации с CLI на устройствах Cisco
9. Протокол TACACS+. Задачи и характеристики протокола
10. Протокол RADIUS. Задачи и характеристики протокола
11. Аутентификация средствами протокола TACACS+. Конфигурирование протокола на устройствах Cisco
12. Аутентификация средствами протокола RADIUS. Конфигурирование протокола на устройствах Cisco
13. Аутентификация с 802.1X
14. Управление доступом в хранилищах данных информационных и аналитических систем.
15. Иерархия прав доступа. Создание ролей.

Примерный перечень вопросов к экзамену. Семестр В

1. Виды привилегий. Операторы представления привилегий.
2. Управление паролями в хранилищах данных информационных и аналитических систем. Операторы отмены привилегий
3. Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.
4. Защита межсетевого взаимодействия в информационных и аналитических системах. Топологии виртуальных частных сетей.
5. Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Remote-Access VPN
6. Защита межсетевого взаимодействия в информационных и аналитических системах. Компоненты Site-to-Site VPN
7. Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол IPSec.
8. Протокол IPSec.Обеспечение конфиденциальности в информационных и аналитических системах.
9. Протокол IPSec.Обеспечение целостности в информационных и аналитических системах.
10. Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол AH. Особенности применения
11. Защита межсетевого взаимодействия в информационных и аналитических системах. Протокол ESP. Особенности применения

12. Команды и алгоритм конфигурирования Site-to-Site VPN на устройствах Cisco
13. Команды и алгоритм конфигурирования Remote-Access VPN на устройствах Cisco
14. Политики ISAKMP. Конфигурирование Pre-Shared Key
15. Протоколы защищенного удаленного доступа в информационных и аналитических системах.
16. Конфигурирование протоколов защищенного удаленного доступа в информационных и аналитических системах.
17. Инфраструктура PKI. Задачи PKI
18. Особенности применения ЭП в информационных и аналитических системах.
19. Криптографические стандарты PKI
20. Топологии PKI

5.3. Самостоятельная работа обучающегося.

Примерные вопросы и задания для самостоятельной работы студентов

Семестр А

1. Общая структура информационных и аналитических систем.
2. Базовые информационные процессы в информационных и аналитических системах.
3. Аналитические системы безопасности: понятия и задачи
4. Современные методы защиты информации в информационных и аналитических системах;
5. Методики выявления основных угрозы безопасности информации, в информационных и аналитических системах;
6. Построение модели нарушителя в информационных и аналитических системах;
7. Защитные механизмы информационной безопасности информационных и аналитических системах;
8. Практика использования информационно-аналитические систем безопасности в профессиональной деятельности;
9. Направления и тенденции совершенствования в вопросах безопасности современных информационно-аналитических систем

Семестр В

1. Регламенты работы с информационно-аналитическими системами
2. Комплект положений, инструкций и других организационно-распорядительных документов для информационно-аналитических системам
3. организационные проблемы информационной безопасности информационно-аналитических систем
4. Технические проблемы информационной безопасности информационно-аналитических систем
5. Требования к организации и функционированию информационно-аналитических систем
6. Модельное представление информационно-аналитических систем
7. Защищенные каналы передачи информации. ESP в туннельном режиме. SSL
8. Защищенные каналы передачи информации. Протокол рукопожатия (SSL HP).
9. Честный обмен цифровыми подписями и его приложения. Схема Asokan - Slioup – Waidner

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*		
1. Кугаевских, А. В. Проектирование информационных систем. Системная и бизнес-аналитика: учебное пособие: [16+] / А. В. Кугаевских; Новосибирский государственный технический университет. – Новосибирск, 2018. – 256 с– ISBN 978-5-7782-3608	2018	https://biblioclub.ru/index.php?page=book&id=573827 (дата обращения: 11.09.2021)
2. Информационно-аналитические системы финансового мониторинга: учебное пособие по курсу «Информационно-аналитические системы и модели»: [16+] / А. Н. Целых, А. А. Целых, Э. М. Котов, М. В. Князева. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2018. – 112 с.– ISBN 978-5-9275-2588-1	2018	https://biblioclub.ru/index.php?page=book&id=499530 (дата обращения: 11.09.2021)
3. Макаров, Р. И. Анализ и синтез информационных систем: учеб. пособие / Р. И. Макаров, Е. Р. Хорошева; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2019. – 251 с. – ISBN 978-5-9984-1001-7.	2019	http://dspace.www1.vlsu.ru/handle/123456789/7569
4. Монахова, Г. Е. ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ. Визуализация многомерных пространственных данных средствами геоинформационных систем: учеб. пособие / Г. Е. Монахова, М. М. Монахова; под ред. проф. М. Ю. Монахова; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2019. – 392 с. – ISBN 978-5-9984-1083-3.	2019	http://dspace.www1.vlsu.ru/handle/123456789/8324
Дополнительная литература		
1. Алдохина, О. И. Информационно-аналитические системы и сети: учебное пособие / О. И. Алдохина, О. Г. Басалаева– Кемерово: Кемеровский государственный университет культуры и искусств (КемГУКИ), 2010. – Ч.1. Информационно-аналитические системы. – 148 с.	2010	https://biblioclub.ru/index.php?page=book&id=227684 (дата обращения: 11.09.2021)
2. Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации: учебное пособие / С. И. Козьминых; Финансовый университет при Правительстве Российской Федерации. – Москва: Юнити-Дана, 2020. – 544 с. – ISBN 978-5-238-03200-9	2020	https://biblioclub.ru/index.php?page=book&id=615695 (дата обращения: 11.09.2021)
3. Березовская, Е. А. Системы поддержки принятия решений: учебное пособие : [16+] / Е. А. Березовская, С. В. Крюков ; Южный федеральный университет. – Ростов-на-Дону; Таганрог: Южный федеральный университет, 2020. – 128 с. – ISBN 978-5-9275-3567-5	2020	https://biblioclub.ru/index.php?page=book&id=612165 (дата обращения: 11.09.2021)

6.2. Периодические издания

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.
3. Ежемесячный теоретический и прикладной научно-технический журнал «Информационные технологии». Режим доступа http://novtex.ru/IT/.

4. «Журнал сетевых решений/LAN» -Режим доступа: http://www.osp.ru/lan/current;
5. Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: http://www.delpress.ru/

6.3. Интернет-ресурсы

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
2. Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
3. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
4. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.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 старший преподаватель кафедры ИЗИ

Матвеева А.П._____/Матвеева А.П./

Рецензент: Заместитель руководителя РАЦ ООО «ИнфоЦентр» к.т.н. Вертилевский Н.В_____

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 14 от 28.06.22 года
Заведующий кафедрой_ д.т.н., профессор_____/М.Ю.Монахов/

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

Протокол № 14 от 28.06.22 года
Председатель комиссии _ д.т.н., профессор_____/М.Ю.Монахов/

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ 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/__

(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ 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/__

(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

Безопасность информационно-аналитических систем

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 _____/__/М.Ю. Монахов/_____

Подпись *ФИО*