

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий



УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
_____ Турилова Е.А.
"___" _____ 20__ г.

Программа дисциплины
Защищенные информационные системы

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль) подготовки: Математические методы и программные технологии защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО
2. Место дисциплины (модуля) в структуре ОПОП ВО
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
 - 4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)
 - 4.2. Содержание дисциплины (модуля)
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
6. Фонд оценочных средств по дисциплине (модулю)
7. Перечень литературы, необходимой для освоения дисциплины (модуля)
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)
12. Средства адаптации преподавания дисциплины (модуля) к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья
13. Приложение №1. Фонд оценочных средств
14. Приложение №2. Перечень литературы, необходимой для освоения дисциплины (модуля)
15. Приложение №3. Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Программу дисциплины разработал(а)(и): старший преподаватель, к.н. Максютин С.В. (Кафедра Интеллектуальной робототехники, Институт информационных технологий и интеллектуальных систем), Sergey.Maksyutin@kpfu.ru

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- модели нарушителей и политик безопасности;
- методы обнаружения вторжений в АС;
- методы безопасного использования коммуникационных сетей общего доступа при построении защищенных АС;
- основные принципы применения аппаратных и программных средств обеспечения ИБ;
- типовые требования безопасности к защищенным АС;

Должен уметь:

- решать задачи проектирования защищенных АС;
- применять современные программные и аппаратные средства защиты информации;
- классифицировать и оценивать угрозы ИБ для защищенного объекта;

Должен владеть:

- навыками разработки комплексной инфраструктуры защищенной информационной системы;
- навыками базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации: файрволов, интерактивных детекторов атак, защищенных доменных сервисов;
- навыками работы с ведущими программными и аппаратными комплексными средствами защиты информации;

Должен демонстрировать способность и готовность:

- выявления угроз информационной безопасности на объекте;
- разработки проектов нормативных и правовых актов предприятия, учреждения, организации, регламентирующих деятельность по обеспечению ИБ на базе защищенного объекта;
- анализа достаточности мер по обеспечению ИБ.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.О.04 Дисциплины (модули)" основной профессиональной образовательной программы 10.04.01 "Информационная безопасность (Математические методы и программные технологии защиты информации)" и относится к обязательной части ОПОП ВО.

Осваивается на 1 курсе в 2 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) на 108 часа(ов).

Контактная работа - 72 часа(ов), в том числе лекции - 36 часа(ов), практические занятия - 36 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 36 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет во 2 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Се- местр	Виды и часы контактной работы, их трудоемкость (в часах)						Само- стоя- тель- ная ра- бота
			Лекции, всего	Лекции в эл. форме	Практи- ческие занятия, всего	Практи- ческие в эл. форме	Лабора- торные работы, всего	Лабора- торные в эл. форме	
1.	Тема 1. Основные понятия защищенных информационных систем. Общие принципы построения защищенных информационных систем.	2	4	0	0	0	0	0	8
2.	Тема 2. Архитектура информационных систем на основе баз данных. Технологии проектирования баз данных.	2	4	0	0	0	0	0	8
3.	Тема 3. Разграничения доступа к ресурсам информационной системы.	2	2	0	0	0	0	0	4
4.	Тема 4. Средства обеспечения целостности информационных систем на основе баз данных. Средства обеспечения конфиденциальности информации в системах на основе баз данных.	2	4	0	0	0	0	0	8
5.	Тема 5. Способы хранения конфиденциальной информации	2	2	0	0	0	0	0	4
6.	Тема 6. Основные направления защиты информации. Организационные меры защиты информации в организации.	2	4	0	0	0	0	0	8
7.	Тема 7. Классификация firewall'ов. Их политики. Типы окружений firewall'ов. Политика безопасности firewall'a.	2	6	0	0	0	0	0	12
8.	Тема 8. Системы обнаружения атак.	2	2	0	0	0	0	0	4
9.	Тема 9. Безопасное использование службы доменных имен (DNS)	2	2	0	0	0	0	0	4
10.	Тема 10. Обеспечение безопасности WEB-серверов. Безопасность WEB-ориентированного контента.	2	4	0	0	0	0	0	8
11.	Тема 11. Технологии аутентификации и шифрования.	2	2	0	0	0	0	0	4
	Итого		36	0	0	0	0	0	72

4.2 Содержание дисциплины (модуля)

Тема 1. Основные понятия защищенных информационных систем. Общие принципы построения защищенных информационных систем.

Понятие 'информационная система'. Концепция безопасности информационной системы. Цели обеспечения информационной безопасности. Санкционированный и несанкционированный доступ. Угрозы безопасности и каналы реализации угроз. Уровни защиты информации. Стандарты безопасности. Классы защищенности информационных систем. Нормативная база Российской Федерации. Современная доктрина информационной безопасности Российской Федерации.

Тема 2. Архитектура информационных систем на основе баз данных. Технологии проектирования баз данных.

Трехуровневая архитектура информационных систем на основе баз данных. Модели баз данных информационных систем. Структура баз данных информационных систем. Целостность реляционных данных. Основные этапы проектирования баз данных. Технологии проектирования на основе нормализации. Технологии проектирования на основе модели. Сущность-связь.

Тема 3. Разграничения доступа к ресурсам информационной системы.

Основные понятия систем разграничения доступа. Сущность и определение политики безопасности. Основные типы политик безопасности: мандатные, ролевые, контроля целостности информационных ресурсов, избирательного разграничения доступа. Субъектно-объектная модель информационной системы.

Тема 4. Средства обеспечения целостности информационных систем на основе баз данных. Средства обеспечения конфиденциальности информации в системах на основе баз данных.

Угрозы целостности информации. Способы противодействия. Понятие и основные свойства транзакций. Механизм блокировок. Декларативная и процедурная ссылочные целостности. Способы поддержания ссылочной целостности. Триггеры и правила. Угрозы конфиденциальности информации. Средства идентификации и аутентификации в СУБД. Средства управления доступом. Виды привилегий. Использование механизма ролей. Метки безопасности. Использование представлений для обеспечения конфиденциальности информации.

Тема 5. Способы хранения конфиденциальной информации

Положение о конфиденциальной информации в электронном виде. Контентная категоризация. Классификация информации по уровню конфиденциальности. Метки документов. Способы хранения конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация.

Тема 6. Основные направления защиты информации. Организационные меры защиты информации в организации.

Защита документов. Защита каналов утечки конфиденциальной информации. Мониторинг действий пользователей. Классификация внутренних нарушителей: неосторожные, манипулируемые, саботажники, нелояльные, мотивированные извне. Другие градации. Кадровая политика. Определение прав локальных пользователей. Стандартизация программного обеспечения. Организация процедуры хранения физических носителей информации. Определение уровней контроля информационных потоков. Режимы архива, сигнализации, активной защиты.

Тема 7. Классификация firewall'ов. Их политики. Типы окружений firewall'ов. Политика безопасности firewall'a.

Классификация. Установление TCP соединения. Пакетные фильтры, набор правил. Пограничные роутеры. Stateful Inspection и Host-based firewall'ы. Персональные firewall'ы и их персональные устройства. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Гибридные технологии firewall'ов. Трансляция сетевых адресов (NAT). Статическая и скрытая трансляция NAT. Принцип построения окружения firewall'a. DMZ-сети. Конфигурация с одной DMZ-сетью. Service Leg конфигурация. Конфигурация с двумя DMZ-сетями. Виртуальные частные сети. Расположение VPN-серверов. Интранет. Экстранет. Компоненты инфраструктуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях. Внешне доступные серверы. VPN и Dial-in серверы. Внутренние серверы. DNS-серверы. SMTP-серверы. Политика firewall'a. Реализация его набора правил. Тестирование политики firewall'a. Возможные подходы к эксплуатации firewall'a. Сопровождение firewall'a и управление им. Физическая безопасность окружения firewall'a. Администрирование firewall'a. Стратегия восстановления после сбоев. Возможность создания логов firewall'a. Инциденты безопасности.

Тема 8. Системы обнаружения атак.

Понятие системы обнаружения атак (IDS). Типы и базовая структура IDS. Совместное расположение Host и Target. Разделение Host и управления. Полностью распределенное управление. Network-based IDS, Host-based IDS, Application-based IDS. Анализ, выполняемый IDS. Определение злоупотреблений. Активные и пассивные ответные действия. Использование SNMP TRAPS. Системы анализа и оценки уязвимостей. Host-based и Network-based анализ уязвимостей. Способы взаимодействия сканера уязвимостей и IDS.

Тема 9. Безопасное использование службы доменных имен (DNS)

Безопасность DNS. Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности. Основные механизмы безопасности для сервисов DNS. Данные

DNS и ПО DNS. Name-серверы. Авторитетные и кэширующие Name-серверы. Resolver'ы.

Транзакции DNS. Запрос/ответ DNS. Зонная пересылка. Динамические обновления.

Безопасность окружения DNS. Угрозы для ПО и данных DNS.

Тема 10. Обеспечение безопасности WEB-серверов. Безопасность WEB-ориентированного контента.

Причины уязвимости WEB сервера. Планирование развертывания WEB сервера.

Безопасное инсталлирование и конфигурирование используемой ОС. Удаление или

запрещение ненужных сервисов и приложений. Управление ресурсами на у

ровне ОС. Альтернативные платформы для web- сервера. Использование

Appliances для web?сервера. Специально усиленные ОС и web серверы. Тестирование безопасности ОС. Безопасное инсталлирование и конфигурирование web сервера.

Соответствующий список действий. Разграничение доступа для ПО web?сервера.

Управление доступом к директории содержимого web? сервера. Публикации информации на web-сайтах. Обеспечение безопасности технологий создания активного содержимого.

URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента.

Уязвимости технологий создания содержимого на стороне сервера. Необходимые действия для обеспечения безопасности web-содержимого.

Тема 11. Технологии аутентификации и шифрования.

Требования к аутентификации и шифрованию. Аутентификация, основанная на

IP-адресе. Basic и Digest аутентификации. SSL/TLS. Возможности и слабые места

SSL/TLS. Пример SSL/TLS сессии. Схемы шифрования SSL/TLS. Список действий при

использовании технологий аутентификации и шифрования. Firewall прикладного уровня

для Web: ModSecurity.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства науки и высшего образования Российской Федерации от 6 апреля 2021 года №245)

Письмо Министерства образования Российской Федерации №14-55-99бин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);

- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;

- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Cisco Learning Network - <https://learningnetwork.cisco.com/index.jsps>

IT eBooks Group - <http://it-ebooks.info>

Telecommunication technologies - <http://book.itpe.ru>

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	Подготовка к лекционному занятию включает повторение лекционного материала предыдущего занятия по соответствующей теме. В ходе лекционных занятий вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой - в ходе подготовки к практическим занятиям изучить основную литературу, ознакомиться с дополнительной литературой. При этом учесть рекомендации преподавателя и требования учебной программы.

Вид работ	Методические рекомендации
практические занятия	<p>Лабораторные работы составляют важную часть профессиональной подготовки студентов. Они направлены на экспериментальное подтверждение теоретических положений и формирование учебных и профессиональных практических умений. Выполнение студентами лабораторных работ направлено на: - обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплин; - формирование необходимых профессиональных умений и навыков; Методические указания по проведению лабораторных работ разрабатываются на срок действия рабочей программы дисциплины и включают: - заглавие, в котором указывается вид работы (лабораторная), ее порядковый номер, объем в часах и наименование; - цель работы; - предмет и содержание работы; - порядок (последовательность) выполнения работы; - общие правила оформления работы; - контрольные вопросы и задания; - список литературы (по необходимости). Состав заданий для лабораторной работы таков, чтобы за отведенное время они могли быть качественно выполнены большинством студентов. Необходимыми структурными элементами лабораторной работы, помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы. Выполнению лабораторных работ предшествует проверка знаний студентов ? их теоретической готовности к выполнению задания. Порядок проведения лабораторных работ в целом совпадает с порядком проведения практических занятий. Помимо собственно выполнения работы для каждой лабораторной работы предусмотрена процедура защиты, в ходе которой преподаватель проводит устный или письменный опрос студентов для контроля понимания выполненных ими измерений, правильной интерпретации полученных результатов и усвоения ими основных теоретических и практических знаний по теме занятия.</p>
самостоятельная работа	<p>Основными формами самостоятельной работы студентов являются: - формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.); - подготовка к практическим занятиям (подготовка сообщений, докладов, заданий); - углубленный анализ рекомендованной научно-методической литературы.</p>
зачет	<p>Подготовка к зачету заключается в изучении и тщательной проработке студентом учебного материала дисциплины с учётом учебников, лекционных и семинарских занятий, сгруппированном в виде контрольных вопросов. Готовиться к зачету необходимо последовательно, с учетом контрольных вопросов, разработанных преподавателем. Следует определить место каждого контрольного вопроса в соответствующем разделе темы учебной программы, а затем прочитать и осмыслить рекомендованные научные работы, соответствующие разделы рекомендованных учебников. При этом полезно делать хотя бы самые краткие выписки и заметки. Работу над темой можно считать завершённой, если студент может ответить на все контрольные вопросы и дать определение понятий по изучаемой теме. Для обеспечения полноты ответа на контрольные вопросы и лучшего запоминания теоретического материала рекомендуется составлять план ответа на контрольный вопрос. Это позволит сэкономить время для подготовки непосредственно перед зачетом за счет обращения не к литературе, а к своим записям</p>

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:
- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;
- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.04.01 "Информационная безопасность" и магистерской программе "Математические методы и программные технологии защиты информации".

*Приложение 2
к рабочей программе дисциплины (модуля)
Б1.О.04 Защищенные информационные системы*

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Математические методы и программные технологии защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

Основная литература:

Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785940747680.html>

Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: НИЦ ИНФРА-М, 2016. - 118 с. - Режим доступа: <http://znanium.com/bookread2.php?book=507334>

Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с. ISBN 978-5-8199-0331-5 - Режим доступа: <http://znanium.com/catalog/product/423927>

Дополнительная литература:

Архитектура и проектирование программных систем: Монография / С.В. Назаров. - М.: НИЦ Инфра-М, 2013. - 351 с. - Режим доступа: <http://znanium.com/bookread.php?book=353187>

Управление качеством программного обеспечения: Учебник / Б.В. Черников. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 240 с. - Режим доступа: <http://znanium.com/bookread.php?book=256901>

Васильев, В.И. Интеллектуальные системы защиты информации. [Электронный ресурс] : учеб. пособие - Электрон. дан. - М. : Машиностроение, 2013. - 172 с. - Режим доступа: <http://e.lanbook.com/book/5792> - Загл. с экрана.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.0.04 Защищенные информационные системы

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Математические методы и программные технологии защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.