Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

И.о директора ИКИТ
_____ Д.В. Капулин
«29» апреля 2022 г.

Институт космических
и информационных технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Методы и системы защиты информации, информационная безопасность

Группа научных специальностей 2.3. Информационные технологии и телекоммуникации

Научная специальность 2.3.6 Методы и системы защиты информации, информационная безопасность

Красноярск 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

составлена в соответствии с Федеральными государственными требованиями

Группа научных специальностей /научная специальность
2.3. Информационные технологии и телекоммуникации / 2.3.6 Методы и системы защиты информации, информационная безопасность

Программу составил
_____ Вайнштейн В.И.

Рабочая программа обсуждена на заседании кафедры (выпускающая) Прикладной математики и компьютерной безопасности
«1» апреля 2022 г. протокол № 96

Заведующий кафедрой
_____ Кытманов А.А.
«1» апреля 2022 г.

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины.

Дисциплина предназначена для изучения принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

Дисциплина закладывает набор базовых знаний, которые позволят выпускникам адаптироваться в условиях бурного развития информационных технологий. Обучение студентов данному курсу способствует воспитанию у них стремления к постоянному повышению профессиональной компетентности, расширению профессионального кругозора, умения ориентироваться в тенденциях и направлениях развития комплексной защиты информации.

1.2 Задачи изучения дисциплины.

Для достижения поставленной цели сформулированы следующие задачи:

– получение теоретических знаний по реализации практических методов, предназначенных для проведения исследований в области информационной безопасности;
– получение практических навыков проведения исследований в области информационной безопасности;
– получение первичных навыков по сбору и анализу нормативно-правовых документов РФ в области обеспечения информационной безопасности.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения программы аспирантуры.

В результате изучения дисциплины аспиранты должны:

знать: законодательные и правовые основы защиты информации и компьютерных технологий, меры по обеспечению сохранности информации, основные задачи обеспечения безопасности информации в информационных системах; принципы построения систем защиты информации и их основы; основные направления создания защищённых информационных систем, определения и свойства математических объектов, используемых в этой области;

уметь: решать задачи теоретического характера из различных разделов дисциплины, доказывать утверждения, строить примеры основных объектов и понятий.

владеть: математическим аппаратом, используемым в системах защиты информации, основными алгоритмами, классификацией способов защиты информации; методами защиты информации от несанкционированного доступа и разрушающих программных воздействий процесса хранения и обработки информации.

1.4 Место дисциплины (модуля) в структуре программы аспирантуры.
Дисциплина относится к образовательной компоненте учебного плана.

1.5 Особенности реализации дисциплины.
Дисциплина реализуется на русском языке.

2 Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад. часов)	Семестр			
		5			
Общая трудоемкость дисциплины	72	72			
Контактная работа с преподавателем:	**46**	**46**			
занятия лекционного типа	30	30			
занятия семинарского типа	16	16			
в том числе: семинары практические занятия	16	16			
другие виды контактной работы					
Самостоятельная работа аспирантов:	**26**	**26**			
изучение теоретического курса (ТО)	26	26			
Вид промежуточной аттестации (зачет, экзамен)	зачет	зачет			

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий).

№ п/п	Модули, темы (разделы) дисциплины	Занятия лекционного типа (акад.час)	Занятия семинарского типа (Семинары и/или Практические занятия (акад.час))	Самостоятельная работа, (акад.час),
1	2	3	4	5
1	Раздел 1. Общие, методологические и правовые аспекты процесса защиты информации	10	5	8
2	Раздел 2. Технические средства защиты информации	10	5	8

3	Раздел 3. Вопросы по специализации, теоретическим основам и современным разработкам в данной области	10	6	10

3.2 Занятия лекционного типа.

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад. часах	
			всего	в том числе в инновационной форме
1	1	Безопасность информационных ресурсов и документирование информации	0.5	-
2	1	Основные задачи обеспечения безопасности информации в информационных системах.	0.5	-
3	1	Государственные информационные ресурсы, персональные данные о гражданах	0.5	-
4	1	Нормативно-правовая база функционирования систем защиты информации	0.5	-
5	1	Российское законодательство по защите информационных технологий	0.5	-
6	1	Коммерческая тайна, промышленный шпионаж	0.5	-
7	1	Банковская тайна, сведения ее составляющие	0.5	-
8	1	Компьютерные преступления и особенности их расследования	0.5	-
9	1	Правовая защита авторских прав	0.5	-
10	1	Проблемы защиты информации в информационных системах	0.5	-
11	1	Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах	0.5	-
12	1	Принципы построения систем защиты информации и их основы	0.5	-
13	1	Нормативно-методическая и научная база системы защиты информации	0.5	-
14	1	Разработка и производство защищенных информационных систем	0.5	-

15	1	Инструментальный базис защиты информации	0.5	-
16	1	Требования к содержанию нормативно-методических документов по защите информации	0.5	-
17	1	Структура и задачи (типовой перечень) органов, выполняющих защиту информации	0.5	-
18	1	Организационно-правовой статус службы информационной безопасности	0.5	-
19	1	Организационно-технические и режимные меры	0.5	-
20	1	Права на доступ к информации. Политика безопасности: организация секретного делопроизводства и мероприятий по защите информации	0.5	-
21	2	Программно-технические методы и средства защиты информации	0.5	-
22	2	Типы несанкционированного доступа и условия работы средств защиты	0.5	-
23	2	Методы и средства криптографической защиты информации (обзорно). Основные понятия и определения. Одноразовая система шифрования	0.5	-
24	2	История криптографической защиты информации: шифры перестановки, шифр перестановки «скитала», шифрующие таблицы, применение магических квадратов, шифры простой замены, квадрат Полибия, шифр Цезаря, шифр Виженра, шифр «двойной квадрат» Уитстона, шифр Вернама, роторные машины	0.5	-
25	2	Шифрование методом гаммирования, методы генерации криптстойких псевдослучайных последовательностей чисел	0.5	-
26	2	Стандарт шифрования данных DES	0.5	-
27	2	Стандарты шифрования данных ГОСТ 28147-89, AES	0.5	-
28	2	Концепция криптосистемы с открытым ключом, однонаправленные функции, комбинированный метод шифрования	0.5	-
29	2	Криптосистемы RSA, Полига—	0.5	-

		Хеллмана и эль-Гамаля		
30	2	Проблема аутентификации данных и электронная цифровая подпись	0.5	-
31	2	Однонаправленные хэш-функции, алгоритмы криптостойкого хеширования SHA-1, MD2, MD5	0.5	-
32	2	Стандарт криптостойкого хеширования ГОСТ 34.11-94	0.5	-
33	2	Однонаправленные хэш-функции на основе симметричных блочных алгоритмов	0.5	-
34	2	Алгоритм ЭП по схемам RSA и эль-Гамаля	0.5	-
35	2	Стандарты ЭП DSA, ЭП ГОСТ 34.10-94 и ГОСТ 34.10-2001	0.5	-
36	2	Аутентификация пользователей без передачи секретной информации в открытом виде	0.5	-
37	2	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов)	0.5	-
38	2	Методы перехвата и навязывания компьютерной информации	0.5	-
39	2	Методы внедрения программных закладок	0.5	-
40	2	Понятие изолированной программной среды	0.5	-
41	3	Угрозы информации, передаваемой и обрабатываемой в компьютерных сетях (обзорно)	0.5	-
42	3	Методы выяснения злоумышленником топологии атакуемой сети	0.5	-
43	3	Атаки, направленные на вывод из строя инфраструктуры сети передачи данных	0.5	-
44	3	Атаки, направленные на изменение штатного режима работы сети передачи данных, в т.ч. с нарушением конфиденциальности и целостности передаваемой информации	0.5	-
45	3	Система адресов в сетях передачи данных и атаки на системы аутентификации, основанные на сетевых адресах. Спуфинг адресов канального, сетевого уровней, DNSспуфинг	0.5	-

46	3	Методы и средства защиты информации в компьютерных сетях (обзорно)	0.5	-
47	3	Режимы функционирования межсетевых экранов и их основные компоненты	0.5	-
48	3	Современные программные и программно-аппаратные межсетевые экраны и персональные сетевые экраны, сравнительный их анализ возможностей	0.5	-
49	3	Технология прокси-серверов как средство защиты информации в сетях	0.5	-
50	3	Технология трансляции сетевых адресов (NAT) как средство защиты информации в сетях	0.5	-
51	3	Криптографические технологии защиты информации в компьютерных сетях (обзорно)	0.5	-
52	3	Методы НСД к информации передаваемой по сетям передачи данных	0.5	-
53	3	Средства обеспечения конфиденциальности информации	0.5	-
54	3	Виртуальные частные сети	0.5	-
55	3	Алгоритм обмена ключами Диффи-Хеллмана	0.5	-
56	3	Инфраструктура открытых ключей. Теоретические основы и современное состояние области в России и за рубежом	0.5	-
57	3	Современные программные и программно-аппаратные продукты для криптографической защиты информации в сетях	0.5	-
58	3	Обнаружение сетевых вторжений	0.5	-
59	3	Методы и средства защиты от атак, использующих уязвимости в клиентском сетевом программном обеспечении абонентских станций. Модели ограничения доступа для программного кода (в т.ч. скриптов и апплетов), загружаемого с недоверенных хостов	0.5	-
60	3	Глобализация источников сетевых угроз. Управляемые сети инфицированных хостов в сети	0.5	-

		Интернет. Распределенные атаки из сети Интернет		

3.3 Занятия семинарского типа

№ п/п	№ раздела дисциплины	Наименование занятий[1]	Объем в акад. часах	
			всего	в том числе в инновационной форме
1	1	Безопасность информационных ресурсов и документирование информации	2	-
2	1	Нормативно-правовая база функционирования систем защиты информации	2	-
3	1	Требования к содержанию нормативно-методических документов по защите информации	2	-
4	1	Организационно-технические и режимные меры	2	-
5	2	Методы и средства криптографической защиты информации	2	-
6	2	Шифрование методом гаммирования, методы генерации криптстойких псевдослучайных последовательностей чисел	2	-
7	2	Стандарт шифрования данных DES, ГОСТ	2	-
8	2	Алгоритмы ЭП по схемам RSA, DSA и ГОСТ	2	-
9	3	Угрозы информации, передаваемой и обрабатываемой в компьютерных сетях	2	-
10	3	Методы и средства защиты информации в компьютерных сетях	2	-
11	3	Криптографические технологии защиты информации в компьютерных сетях	2	-
12	3	Инфраструктура открытых ключей	2	-
13	3	Обнаружение сетевых вторжений	2	-

4. Перечень учебно-методического обеспечения для самостоятельной работы аспирантов по дисциплине (модулю)

УМО «Криптографические методы защиты информации», Вайнштейн В.И. https://e.sfu-kras.ru/course/view.php?id=26540

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — М. : Издательство Юрайт, 2018. — 309 с. — (Серия : Бакалавр и магистр. академический курс). — ISBN 978-5-534-04732-5. — Режим доступа : www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E.

2. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана. (http://www.iprbookshop.ru/63594.html)

3. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем Учебник для вузов в 2-х томах (с грифом Минобразования и науки РФ). Том 1 – Угрозы, уязвимости, атаки и подходы к защите.). Том 2 – Средства защиты в сетях.- М.: Горячая линия-Телеком, 2013, 538 с. Режим доступа: http://www.iprbookshop.ru/63594.html

4. Мельников, Д.А. Информационная безопасность открытых систем [Электронный ресурс] : учеб. — Электрон. дан. — Москва : ФЛИНТА, 2014. — 448 с. — Режим доступа: https://e.lanbook.com/book/48368. — Загл. с экрана.

5. Галатенко, В.А. Стандарты информационной безопасности [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : Национальный Открытый Университет "ИНТУИТ", 2016. — 307 с. — Режим доступа: https://e.lanbook.com/book/100511. — Загл. с экрана.

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

– Университетская информационная система «РОССИЯ» https://uisrussia.msu.ru
– Справочно-правовая система «Консультант+» http://www.consultant-urist.ru
– Справочно-правовая система «Гарант» http://www.garant.ru
– База данных Web of Science https://apps.webofknowledge.com/
– База данных Scopus https://www.scopus.com
– Портал открытых данных Российской Федерации https://data.gov.ru
– База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata
– База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/
– База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestrprofessionalnykh-standartov/
– Базы данных Министерства экономического развития РФ http://www.economy.gov.ru
– База открытых данных Росфинмониторинга http://www.fedsfm.ru/opendata

– Электронная база данных «Издательство Лань» https://e.lanbook.com
– Электронная библиотечная система «IPRbooks» http://www.iprbookshop.ru
– База данных «Электронно-библиотечная система «ЭБС ЮРАЙТ» https://www.biblioonline.ru
– Федеральная государственная информационная система «Национальная электронная библиотека» https://нэб.рф
– Национальный портал онлайн обучения «Открытое образование» https://openedu.ru
– Электронная база данных "Polpred.com Обзор СМИ" https://www.polpred.com
– Официальный сайт Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru/

7. Методические указания для аспирантов по освоению дисциплины (модуля)

К современному специалисту общество предъявляет достаточно широкий перечень требований, среди которых немаловажное значение имеет наличие у выпускников определенных способностей и умений самостоятельно добывать знания из различных источников, систематизировать полученную информацию, давать оценку конкретной ситуации. Формирование такого умения происходит в течение всего периода Вашего обучения через участие в практических занятиях, выполнение контрольных заданий и тестов. При этом Ваша самостоятельная работа играет решающую роль в ходе всего учебного процесса.

Успешное освоение компетенций, формируемых данной учебной дисциплиной, предполагает оптимальное использование Вами времени самостоятельной работы. Целесообразно посвящать до 20 минут изучению конспекта лекции в тот же день после лекции и за день перед лекцией. Теоретический материал изучать в течение недели до 2 часов, а готовиться к практическому занятию по дисциплине до 1.5 часов.

Для понимания материала учебной дисциплины и качественного его усвоения Вам рекомендуется такая последовательность действий:

– после прослушивания лекции и окончания учебных занятий, при подготовке к занятиям следующего дня нужно сначала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры;

– при подготовке к лекции следующего дня нужно просмотреть текст предыдущей лекции, подумать о том, какая может быть тема следующей лекции;

– в течение недели выбрать время для работы с литературой по учебной дисциплине в библиотеке и для решения задач;

– при подготовке к практическим занятиям повторить основные понятия и формулы по теме домашнего задания, изучить примеры;

– решая упражнение или задачу, предварительно понять, какой теоретический материал нужно использовать; наметить план решения, попробовать на его основе решить 1-2 аналогичные задачи. При решении задач всегда необходимо комментировать свои действия и не забывать о содержательной интерпретации.

Рекомендуется использовать методические указания и материалы по учебной дисциплине, текст лекций, а также электронные пособия, имеющиеся в системе LMS Moodle.

Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекций Вами изучаются и книги по данной учебной дисциплине. Полезно использовать несколько учебников, однако легче освоить курс, придерживаясь одного учебника и конспекта.

Рекомендуется, кроме «заучивания» материала, добиться понимания изучаемой темы дисциплины. С этой целью после прочтения очередной главы желательно выполнить несколько простых упражнений на соответствующую тему. Кроме того, очень полезно мысленно задать себе и попробовать ответить на следующие вопросы: о чем эта глава, какие новые понятия в ней введены, каков их смысл. При изучении теоретического материала всегда полезно выписывать формулы и графики.

При подготовке к промежуточной аттестации необходимо освоить теоретические положения данной дисциплины, разобрать определения всех понятий и постановки моделей, описывающих процессы, рассмотреть примеры и самостоятельно решить несколько типовых задач из каждой темы. Дополнительно к изучению конспектов лекций необходимо пользоваться учебниками по учебной дисциплине.

При выполнении домашних заданий необходимо сначала прочитать теорию и изучить примеры по каждой теме. Решая конкретную задачу, предварительно следует понять, что требуется от Вас в данном случае, какой теоретический материал нужно использовать, наметить общую схему решения. Если Вы решали задачу «по образцу» рассмотренного на аудиторном занятии или в методическом пособии примера, то желательно после этого обдумать процесс решения и попробовать решить аналогичную задачу самостоятельно.

Учебно-методические материалы для самостоятельной работы аспирантов из числа инвалидов и лиц с ограниченными возможностями здоровья представляются в формах, адаптированных к ограничениям их здоровья и восприятия информации в зависимости от нозологии:

Для лиц с нарушениями зрения:

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

Перечень необходимого программного обеспечения:

MS Office, Windows (или аналоги).

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Учебные аудитории для проведения занятий лекционного типа (Мебель: учебная мебель Технические средства: экран, проектор, компьютер).

Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации(Мебель: учебная мебель Технические средства: экран, проектор, компьютер).

Читальный зал. Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Технические средства: компьютерная техника с подключением к информационнокоммуникационной сети «Интернет» и доступом в электронную информационнообразовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi).