Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Рабочая программа дисциплины

Организационное и правовое обеспечение информационной безопасности

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности.

ПК-2 Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-4.2 Учитывает основные требования информационной безопасности.

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.

ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.

2. Задачи освоения дисциплины

– ознакомить студентов с основными законодательными и подзаконными актами в области защиты информации;

– научить использовать нормативные правовые акты и методические документы в области информационной безопасности, в том числе регулирующие вопросы организации лицензирования и оценки соответствия в Российской Федерации;

– обучить анализу и оценке угроз информационной безопасности, в частности, связанных с утечкой информации по техническим каналам утечки информации, а также выявляемых при разработке системы защиты информации в информационных системах персональных данных;

– обучить общим принципам организации защиты информации с применением модели угроз и модели нарушителя.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль «Введение в специализацию».

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Третий семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуется знать общие методы обеспечения информационной безопасности и основные типы средств обеспечения информационной безопасности.

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Введение

Введение в правовые основы. Информация как объект права. Правовое регулирование в области защиты информации. Органы исполнительной власти, осуществляющие регулирование. Закон об информации, информационных технологиях и защите информации. Регулирование использования международной сети Интернет.

Тема 2. Лицензирование и оценка соответствия

Лицензирование в области защиты информации. Формы оценки соответствия. Сертификация средств защиты информации по требованиям безопасности. Аккредитация. Аттестация объектов информатизации. Нормативные документы ФСБ и ФСТЭК по аттестации.

Тема 3. Технические каналы утечки информации

Технические каналы утечки информации.

Тема 4. Законодательство в области защиты персональных данных

Общие сведения по законодательству в области персональных данных. Закон о персональных данных. Уровни защищенности информационных систем персональных данных. Требования ФСБ по защите информационных систем персональных данных. Требования ФСТЭК по защите информационных систем персональных данных. Модели угроз. Оценка актуальности угроз.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения коллоквиумов, опросов, выполнения заданий самостоятельной работы, и фиксируется в форме контрольной точки не менее одного раза в семестр.

Занятия по дисциплине проводятся в классической форме в виде лекций:

– лекции в виде классического изложения преподавателем основного теоретического материала. В начале лекции проводится быстрый устный опрос по пройденному материалу, который необходим для проведения текущей лекции. В конце лекции подводится краткий итог (перечисление) основных положений, пройденных на лекции. По итогу прохождения основных тематических блоков дисциплины предусмотрено проведение опросов в письменном виде.

Обязательными при изучении дисциплины «Организационное и правовое обеспечение информационной безопасности» являются следующие виды самостоятельной работы:

– разбор теоретического материала по конспектам лекций, учебным пособиям и научным статьям;

– выполнение заданий по темам лекций.

Для текущего контроля самостоятельной работы студентов в середине семестра предусмотрено проведение коллоквиума по первому и второму разделам дисциплины.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет в третьем семестре осуществляется в письменном виде при условии успешной сдачи коллоквиума. Продолжительность зачета 1 час.

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=9965

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

в) План семинарских / практических занятий по дисциплине.

Не предусмотрены

г) Методические указания по проведению лабораторных работ.

Не предусмотрены

д) Методические указания по организации самостоятельной работы студентов.

Основой обучения является курс лекций, читаемый преподавателем. Для самостоятельной работы и дополнительного расширения круга знаний рекомендуется использовать литературу, приведенную в разделе 12, а также информационные технологии, приведенные в разделе 13.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Федеральное собрание Российской Федерации. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», 2006 г.

– Федеральное собрание Российской Федерации. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», 2006 г.

– Президент Российской Федерации. Указ президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», 2016 г.

– Федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (утвержден Федеральным агентством по техническому регулированию и метрологии). ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» от 27.12.2006 г., 2006 г.

– Федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю»; Общество с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (утвержден Федеральным агентством по техническому регулированию и метрологии). ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» от 18.12.2008 г., 2008 г.

– Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2016. – 474 с.

– Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р. Защита персональных данных в организации. – М.: ФЛИНТА, 2016. – 124 с.

– Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами. – СПб: НИУ ИТМО, 2012. – 416 с.

– Чубукова С.Г. Организационное и правовое обеспечение информационной безопасности. Учебник и практикум. – М.: Юрайт, 2016. – 326 с.

– Правительство Российской Федерации. Постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации», 2012 г.

– Правительство Российской Федерации. Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», 2012 г.

– Правительство Российской Федерации. Постановление Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации», 1995 г.

– Федеральная служба по техническому и экспортному контролю Российской Федерации. Приказ ФСТЭК России от 10.04.2015 № 33 «Об утверждении Правил выполнения отдельных работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке (подтверждению) соответствия в отношении продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, и продукции (работ, услуг), сведения о которой составляют государственную тайну, в установленной ФСТЭК России сфере деятельности», 2015 г.

– Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации Приказ Минцифры России от 29 октября 2020 года № 559 «Об утверждении Административного регламента предоставления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственной услуги по аккредитации удостоверяющих центров и Административного регламента осуществления Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации государственного контроля (надзора) за соблюдением аккредитованными удостоверяющими центрами требований, которые установлены Федеральным законом "Об электронной подписи" и на соответствие которым эти удостоверяющие центры были аккредитованы», 2020 г.

– Государственная техническая комиссия при Президенте Российской Федерации. Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено Гостехкомиссией РФ 25.11.1994), 1994 г.

– Федеральная служба по техническому и экспортному контролю Российской Федерации. Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну», 2021 г.

– Правительство Российской Федерации. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", 2012 г.

– Федеральная служба по техническому и экспортному контролю Российской Федерации. Приказ ФСТЭК России от 18 февраля 2013 года № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", 2013 г.

– Федеральная служба безопасности Российской Федерации. Приказ ФСБ РФ от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», 2014 г.

б) дополнительная литература:

– Мельников В.П., Куприянов А.И. Информационная безопасность. – М.: КНОРУС, 2018. – 268 с.

– Ковалева Н.Н. Информационное право в России. Учебное пособие. – М.: Дашков и КО, 2007. – 360 с.

– Жарова А.К. Право и информационные конфликты в информационно-телекоммуникационной сфере. – М.: Янус, 2016. – 248 с.

– Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки по техническим каналам: Учебное пособие. – М.: Горячая линия-Телеком, 2005. – 416 с.

– Федеральное государственное учреждение «32 Государственный научно-исследовательский испытательный институт Минобороны России»; Федеральное государственное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (утвержден Федеральным агентством по техническому регулированию и метрологии). ГОСТ Р 53112-2008 «Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний» от 18.12.2008 г., 2008 г.

в) ресурсы сети Интернет:

– электронный ресурс: http://www.kremlin.ru/acts/bank

– электронный ресурс: http://pravo.gov.ru

– электронный ресурс: https://docs.cntd.ru

– Общероссийская Сеть КонсультантПлюс Справочная правовая система. http://www.consultant.ru

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

– ЭБС Консультант студента – http://www.studentlibrary.ru/

– Образовательная платформа Юрайт – https://urait.ru/

– ЭБС ZNANIUM.com – https://znanium.com/
– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Останин Сергей Александрович, канд. техн. наук, заведующий кафедрой компьютерной безопасности.