


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

Юридический институт

УТВЕРЖДАЮ:

Директор

 О. И. Андреева

« 05 » 06 20 23 г.

Рабочая программа дисциплины

Информационная безопасность

по направлению подготовки

40.03.01 Юриспруденция

Направленность (профиль) подготовки :

Цифровой юрист

Форма обучения

Очная

Квалификация

Бакалавр

Год приема

2023

Код дисциплины в учебном плане:

Б1.В.05.01

СОГЛАСОВАНО:

Руководитель ОП

 Т.В. Трубникова

Председатель УМК

 С.Л. Лонь

Томск – 2023

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-9 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

ПК-1 Способен осуществлять юридическое обеспечение в сфере информационной безопасности.

УК-8 Способен создавать и поддерживать безопасные условия жизнедеятельности в различных средах для сохранения природной среды и обеспечения устойчивого развития общества.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 9.4 Владеет навыками алгоритмизации, программирования на начальном уровне, может их использовать при осуществлении профессиональной деятельности.

ИПК 1.1 Определяет совместно со специалистами в области информационных технологий угрозы в области информационной безопасности и предлагает юридические решения

ИПК 1.2 Соблюдает в своей профессиональной деятельности основные требования информационной безопасности, в том числе в части обеспечения защиты информации и персональных данных, неразглашения сведений, составляющих охраняемые законом виды профессиональных тайн

ИПК 1.4 Разрабатывает проекты нормативных актов, в том числе локальных в области обеспечения информационной безопасности

ИУК 8.1 Выявляет возможные угрозы для жизни и здоровья в повседневной и профессиональной жизни в условиях чрезвычайных ситуаций в различных средах (природной, цифровой, социальной, эстетической)

ИУК 8.2 Предпринимает необходимые действия по обеспечению безопасности жизнедеятельности в различных средах (природной, цифровой, социальной, эстетической), а также в условиях чрезвычайных ситуаций

2. Задачи освоения дисциплины

освоение общих принципов проектирования и разработки безопасного программного обеспечения, видов уязвимостей, способов защиты от ошибок в программном обеспечении

освоение навыков моделирования угроз в сфере информационной безопасности
знание способов снижения рисков информационной безопасности

освоение законодательной базы Российской Федерации в области информационной безопасности

3. Место дисциплины в структуре образовательной программы

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

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений. Дисциплина входит в модуль «Правовое обеспечение информационной безопасности».

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

Шестой семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим модулям/ дисциплинам: модуль «Цифровая культура», модуль «Работа с данными», модуль «Экономика и предпринимательство»

6. Язык реализации
Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:

-лекции: 12 ч.

-практические занятия: 24 ч.

в том числе практическая подготовка: 2 ч.

Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Основные понятия:

Понятие «безопасность».

Понятия «хакер», «атакующий», «злоумышленник».

Понятия «безопасное программирование», «secure coding» и «defensive programming».

Важность безопасного программирования.

Основные принципы разработки безопасного программного обеспечения (ПО).

Тема 2. Разбор стандарта о разработке безопасного программного обеспечения:

Ключевые моменты.

Разбор предлагаемых мер по защите.

Документы, которые должны быть в наличии: список и содержание.

Соответствие другим нормативным актам и стандартам.

Аспекты, которые не покрывает стандарт.

Аналоги в мире.

Тема 3. Способы снижения рисков информационной безопасности:

Защита инфраструктуры среды разработки ПО.

Разработка безопасного ПО на всех этапах жизненного цикла.

Организация тестирования ПО.

Управление изменениями требований.

Обеспечения конфиденциальности информации, получаемой в ходе разработки и анализа кода, тестирования ПО.

Дизайн и архитектура ПО.

Передача исходного кода ПО третьей стороне.

Тема 4. Классификация и виды уязвимостей:

Классификаторы уязвимостей. Система подсчета рисков уязвимости. Виды уязвимостей.

Тема 5. Механизмы для защиты от ошибок в ПО:

Встроенные в компилятор и фреймворк. Встроенные в операционную систему. Распространенные ошибки.

Тема 6. Проектирование безопасных пользовательских интерфейсов:

Основные принципы.

Распространенные ошибки.

Тема 7. Тестирование кода:

Статический анализ и экспертиза кода.

Функциональное тестирование программы.

Тестирование на проникновение.

Динамический анализ кода.

Фаззинг-тестирование.

Тема 8. Сертификация ПО:

Обоснование необходимости.

Законодательство в мире.

Процедура сертификации ПО в Российской Федерации.

Тема 9. Что делать, если уже есть приложение:

План реагирования на инциденты информационной безопасности.

Средства защиты приложений.

Моделирование угроз.

Проверка на защищенность.

Тема 10. Информационная безопасность компании:

Системы электронного документооборота: защита информации и информационная безопасность.

Фильтрация спама как элемент политики информационной безопасности.

Тема 11. Кибервойны:

Немного из истории.

Принципы ведения Кибервойн.

9. Текущий контроль по дисциплине

Текущий контроль и промежуточная аттестация по модулю осуществляются с применением балльно-рейтинговой системы.

Обучающиеся изучают рекомендованный онлайн-курс (курсы). Результаты освоения онлайн-курса, подтвержденные сертификатом создателя онлайн-курса перезачитываются в качестве текущего контроля по дисциплине «Информационная безопасность». Наличие указанного сертификата является обязательным условием для допуска к промежуточной аттестации по модулю «Информационная безопасность».

10. Порядок проведения и критерии оценивания промежуточной аттестации

Обучающиеся изучают рекомендованный онлайн-курс (курсы). Результаты освоения онлайн-курса, подтвержденные сертификатом создателя онлайн-курса перезачитываются в качестве текущего контроля по дисциплине «Информационная безопасность». Наличие указанного сертификата является обязательным условием для допуска к промежуточной аттестации по модулю «Информационная безопасность».

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - <https://moodle.tsu.ru/course/view.php?id=00000>

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

в) План семинарских / практических занятий по дисциплине.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

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.

б) дополнительная литература:

Жигулин, Г.П. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учеб. пособие — Электрон. дан. — Санкт-Петербург: НИУ ИТМО, 2014. — 173 с. — Режим доступа: <https://e.lanbook.com/book/70952>. — Загл. с экрана.

в) ресурсы сети Интернет:
Common Weakness Enumeration [Электронный ресурс]. Режим доступа:
<https://cwe.mitre.org/index.html>
OWASP Secure Coding Practices-Quick Reference Guide [Электронный ресурс].
Режим доступа: <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/>
– 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 OneNote, 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 занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации, в том числе компьютерные классы.

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

Аудитории для проведения занятий лекционного и семинарского типа индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации в смешанном формате («Актру»).

15. Информация о разработчиках

Трубникова Татьяна Владимировна, к.ю.н., доцент кафедры уголовного процесса, прокурорского надзора и правоохранительной деятельности ЮИ ТГУ..