

1117 2023

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ
Н.Г. ЧЕРНЫШЕВСКОГО»
Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ
Декан факультета
Миронов С.В.



«15» июня 2023 г.

**Рабочая программа дисциплины
Защита программ и данных**

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2023

| Статус | ФИО | Подпись | Дата |
|--------------------------------|------------------|---------|---------------|
| Преподаватель-разработчик | Лобов А. А. | | 15.06.2023 г. |
| Председатель НМК | Кондратова Ю. Н. | | 15.06.2023 г. |
| Заведующий кафедрой | Абросимов М. Б. | | 15.06.2023 г. |
| Специалист Учебного управления | | | |

1. Цели освоения дисциплины

Целями освоения дисциплины «Защита программ и данных» является знакомство с основными методами и средствами обеспечения защиты программ и исходных текстов программ, а также защиты данных, представленных в электронном виде.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к обязательной части Блока 1 «Дисциплины (Модули)» ООП и направлена на формирование у обучающихся общепрофессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Аппаратные средства вычислительной техники», «Компьютерные сети», «Операционные системы», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплины «Модели безопасности компьютерных систем».

Компетенции, сформированные при изучении данной дисциплины, могут быть полезны при изучении дисциплин «Программно-аппаратные средства обеспечения информационной безопасности».

3. Результаты обучения по дисциплине

| Код и наименование компетенции | Код и наименование индикатора (индикаторов) достижения компетенции | Результаты обучения |
|---|---|---|
| ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. | ОПК-9.1.1 знает принципы построения современных операционных систем, компьютерных сетей и систем управления базами данных; ОПК-9.2.1 умеет применять методы защиты информации в операционных системах, компьютерных сетях и системах управления базами данных; ОПК-9.2.3 умеет анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи; ОПК-9.3.1 владеет навыками решения задач профессиональной деятельности с учетом текущего состояния и | Знать основные подсистемы операционных систем, основные компоненты компьютерных сетей и виды их характеристик, основные сетевые службы, принципы работы систем управления базами данных; основные проводные и беспроводные интерфейсы передачи информации, принципы организации защищённого канала связи. Уметь использовать механизмы операционной системы, системного и прикладного программного обеспечения для защиты информации; анализировать новые службы и протоколы передачи информации Владеть навыками |

| Код и наименование компетенции | Код и наименование индикатора (индикаторов) достижения компетенции | Результаты обучения |
|---|---|---|
| | тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации. | администрирования и настройки безопасности систем управления базами данных; навыками исследования структуры компьютерной сети, анализа защищённости компьютерной сети. |
| ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности. | <p>ОПК-13.1.1 знает средства и методы разработки компонент программных и программно-аппаратных средств защиты информации в компьютерных системах;</p> <p>ОПК-13.2.1 умеет разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах;</p> <p>ОПК-13.2.3 умеет формализовать поставленную задачу; работать с интегрированными средами разработки программного обеспечения;</p> <p>ОПК-13.3.1 владеет навыками проведения анализа безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах;</p> <p>ОПК-13.3.3 владеет навыками разработки, отладки, документирования и тестирования программ; навыками использования инструментальных средств отладки и дизассемблирования программного кода;</p> | <p>Знать методы защиты программ и данных в компьютерных системах.</p> <p>Уметь программно реализовывать методы защиты программ и данных; формализовывать поставленную задачу, работать с интегрированными средами разработки программного обеспечения</p> <p>Владеть навыками анализа безопасности компонент программных и программно-аппаратных средств защиты информации в компьютерных системах; навыками и средствами анализа, тестирования, отладки и документирования программ; методами оценки качества программного обеспечения, навыками разработки алгоритмов для решения типовых профессиональных задач.</p> |

| Код и наименование компетенции | Код и наименование индикатора (индикаторов) достижения компетенции | Результаты обучения |
|--------------------------------|---|---------------------|
| | ОПК-13.3.4 владеет методами оценки качества готового программного обеспечения; навыками разработки алгоритмов для решения типовых профессиональных задач. | |

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единицы, 180 часов.

| № п/п | Раздел дисциплины | Семестр | Неделя семестра | Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах) | | | | | Формы текущего контроля успеваемости и (по неделям семестра) Формы промежуточной аттестации (по семестрам) |
|-------|--|---------|-----------------|--|----------------------|----------------------------------|-----|----|--|
| | | | | Лекции | Лабораторные занятия | | ИКР | СР | |
| | | | | | Общая трудоемкость | Из них – практическая подготовка | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1 | Защита приложений от изучения | 8 | 1-4 | 8 | 8 | – | 1 | 19 | Контрольная работа на 16-й неделе |
| 2 | Уязвимости в приложениях | | 5-8 | 8 | 8 | – | 1 | 19 | |
| 3 | Защита данных | | 9-12 | 8 | 8 | – | 1 | 19 | |
| 4 | Защита программ и данных от сетевых атак | | 13-16 | 8 | 8 | – | 1 | 19 | |
| | Промежуточная аттестация – 36 часов | | | | | | | | Экзамен, курсовая работа |
| | ИТОГО – 180 ч. | | | 32 | 32 | – | 4 | 76 | – |

Содержание дисциплины

Защита приложений от изучения. Языки программирования, компиляторы, интерпретаторы и исполнимые файлы. Способы изучения исполнимых файлов: отладка, дизассемблирование, декомпиляция, просмотр памяти приложения. Способы защиты от изучения исполнимых файлов: выявление процесса отладки, обфускация программного кода, использование интерпретаторов, динамическое зашифрование и расшифрование программного кода, использование отдельного аппаратного устройства. Навесные защиты.

Уязвимости в приложениях. Виды уязвимостей приложений и возможных атак. Особенности языков разработки приложений с точки зрения безопасности. Обнаружение уязвимостей в приложении: динамический и статический анализ. Символьное исполнение. Фазинг-тестирование. Тестирование программы на наличие уязвимостей в цикле разработки приложений.

Защита данных. Хранение и передача данных. Основные свойства информации с точки зрения безопасности: доступность, целостность и конфиденциальность. Хеш-функции, имитовставка, помехоустойчивое кодирование, резервное копирование, электронная цифровая подпись. Стеганография, цифровые водяные знаки. Основные атаки на доступность информации и способы противодействия. Способы защиты конфиденциальности данных: криптографические методы, разграничение доступа, квантовая криптография. Системы предотвращения утечек информации.

Защита программ и данных от сетевых атак. Стадии проведения и цели атаки. Обнаружение процесса сканирования сети. Пассивный сбор данных и его выявление. Уязвимости в веб-приложениях, принцип их работы, примеры и способы защиты. Тестирование сетевых приложений. Атака «Человек посередине», её особенности. Туннелирование. Выработка общего ключа. Квантовые вычисления и постквантовая криптография. Протоколы SSL/TLS, SSL-сертификаты, инфраструктура открытых ключей. Схемы разделения секрета.

План лабораторных занятий

На лабораторных занятиях студенты выполняют задания, связанные с закреплением полученного теоретического материала, в том числе с использованием программного обеспечения.

| № занятия | Тема | Задания для лабораторного практикума |
|-----------|--|--------------------------------------|
| 1 | 2 | 3 |
| 1-4 | Защита приложений от изучения | № 1,2 |
| 5-8 | Уязвимости в приложениях | № 3,4,5 |
| 9-12 | Защита данных | № 6,7 |
| 13-16 | Защита программ и данных от сетевых атак | № 8,9,10 |

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких активных и интерактивных форм проведения занятий как интерактивный опрос, диалог, выступления экспертов и специалистов перед студентами, встречи с представителями ведущих отечественных фирм по защите информации, ознакомительные беседы с представителями потенциальных работодателей, использование проблемного и проектного методов, работа в команде.

Иная контактная работа представляет собой индивидуальные консультации, оказываемые очно и дистанционно с использованием информационных и телекоммуникационных технологий с учётом возможностей обучающихся.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве. При этом основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья, т. е. все студенты обучаются в смешанных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты изучают источники, в которых более детально рассматривается материал. Каждому студенту выдается контрольная работа, связанная с практическим изучением методов и средств защиты компьютерных программ и данных, которая выполняется студентом самостоятельно. Контроль текущей успеваемости осуществляется в процессе проведения лабораторных занятий.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольной работы, тесты, контрольные вопросы, вопросы для проведения промежуточной аттестации (экзамен), темы курсовых работ. Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе дисциплины «Защита программ и данных».

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 – Таблица максимальных баллов по видам учебной деятельности

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---------|--------|----------------------|----------------------|------------------------|---------------------------------|----------------------------------|--------------------------|-------|
| Семестр | Лекции | Лабораторные занятия | Практические занятия | Самостоятельная работа | Автоматизированное тестирование | Другие виды учебной деятельности | Промежуточная аттестация | Итого |
| 8 | 10 | 30 | 0 | 20 | 0 | 10 | 30 | 100 |

Программа оценивания учебной деятельности студента

8 семестр

Лекции

Посещаемость, активность за один семестр – от 0 до 10 баллов.

Лабораторные занятия

Выполнение заданий – от 0 до 30 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Выполнение заданий в рамках самостоятельной работы – от 0 до 20 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Выполнение контрольной работы – от 0 до 10 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой экзамен, проводимый в устной форме с предварительной подготовкой студента к ответу.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 24 до 30 баллов;

ответ на «хорошо» оценивается от 18 до 23 баллов;

ответ на «удовлетворительно» оценивается от 10 до 17 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 9 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за восьмой семестр по дисциплине «Защита программ и данных» составляет 100 баллов.

Таблица 2.1 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Защита программ и данных» в оценку (экзамен)

| | |
|---------------|-----------------------|
| 80-100 баллов | «отлично» |
| 60-79 баллов | «хорошо» |
| 40-59 баллов | «удовлетворительно» |
| 0-39 баллов | «неудовлетворительно» |

Курсовые работы у студентов специальности 10.05.01 Компьютерная безопасность в восьмом семестре закреплены за дисциплиной «Защита программ и данных».

Таблица 1.1 – Таблица максимальных баллов по видам учебной деятельности.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---------|--------|----------------------|----------------------|------------------------|---------------------------------|----------------------------------|--------------------------|-------|
| Семестр | Лекции | Лабораторные занятия | Практические занятия | Самостоятельная работа | Автоматизированное тестирование | Другие виды учебной деятельности | Промежуточная аттестация | Итого |
| 8 | 0 | 0 | 0 | 40 | 0 | 20 | 40 | 100 |

Программа оценивания учебной деятельности студента

8 семестр

Лекции

Не предусмотрено.

Лабораторные занятия

Не предусмотрено.

Практические занятия

Не предусмотрено.

Самостоятельная работа

Оценивается сбор, анализ и систематизация теоретической, научно-практической информации по тематике курсовой работы; обоснованный выбор методов и инструментальных средств для проведения вычислительного эксперимента; планирование, проведение и анализ результатов вычислительного эксперимента, грамотность в оформлении – от 0 до 40 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Оценивается планомерная работа над курсовой работой во время семестра, регулярные консультации с научным руководителем, своевременное представление курсовой работы на защиту – от 0 до 10 баллов; участие в научных мероприятиях по тематике курсовой работы или ином публичном представлении результатов курсовой работы, в том числе участие в создании объектов интеллектуальной собственности; публикация результатов исследований выполненных в рамках курсовой работы – от 0 до 10 баллов.

Промежуточная аттестация – зачёт с оценкой

Включает в себя соблюдение требований к оформлению текста курсовой работы; подготовка презентации выступления для защиты курсовой работы; грамотность и логичность выступления с результатами работы на защите курсовой работы; исчерпывающие, правильные и уверенные ответы на вопросы в ходе защиты курсовой работы.

При проведении промежуточной аттестации

результат работы на «отлично» / «зачтено» оценивается от 32 до 40 баллов;

результат работы на «хорошо» / «зачтено» оценивается от 24 до 31 баллов;

результат работы на «удовлетворительно» / «зачтено» оценивается от 16 до 23 баллов;

результат работы на «неудовлетворительно» / «не зачтено» оценивается от 0 до 15 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за восьмой семестр по курсовой работе составляет 100 баллов.

Таблица 2.2 Таблица пересчета полученной студентом суммы баллов по курсовой работе в оценку (зачёт с оценкой)

| | |
|---------------|------------------------------------|
| 80–100 баллов | «отлично» / зачтено |
| 60–79 баллов | «хорошо» / зачтено |
| 40–59 баллов | «удовлетворительно» / зачтено |
| 0–39 баллов | «неудовлетворительно» / не зачтено |

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1) Бабушкин, В.М. Разработка защищенных программных средств информатизации производственных процессов предприятия: учебное пособие / В.М. Бабушкин, М.В. Тумбинская. – Казань: Изд-во КНИТУ-КАИ, 2020. – 256 с. ISBN 978-5-7579-2463-2 URL: <https://e.lanbook.com/book/193486>

2) Буйневич, М.В. Защита программ и данных. Часть 1. Способы анализа : учебное пособие / М.В. Буйневич, К.Е. Израилов, А.В. Красов // СПбГУТ. – СПб., 2020. – 72 с. URL: <https://e.lanbook.com/book/180081>

3) Буйневич, М.В. Защита программ и данных. Часть 2. Способы защиты от анализа : учебное пособие / М.В. Буйневич, К.Е. Израилов, А.В. Красов // СПбГУТ. – СПб., 2020. – 52 с. URL: <https://e.lanbook.com/book/180082>

4) Федосеев, В. А. Цифровые водяные знаки и стеганография: учеб. Пособие / В.А. Федосеев; 2-е изд., испр. И доп. – Самара: Изд-во Самарского университета, 2019. – 144 с. – 15 ил. URL: <https://e.lanbook.com/book/148589> ISBN 978-5-7883-1370-2

5) Юрин, И. Ю. Теоретические и практические основы защиты информации [Электронный ресурс]: учеб. пособие / И. Ю. Юрин. Саратов, 2012. 32 с. URL: http://library.sgu.ru/uch_lit/620.pdf (дата обращения: 01.06.2023). Загл. с экрана. Яз. рус.

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: Программный комплекс СКЗИ «КриптоПро CSP» версии 5.0, программный комплекс СКЗИ «КриптоПро CSP» версии 5.0 на сервер, Удостоверяющий центр «КриптоПро УЦ» версии 2.0 класс КС2.

2) Свободное программное обеспечение: VirtualBox или KVM, ОС на базе ядра Linux (Simply Linux, Ubuntu Desktop, Ubuntu Server), дистрибутив Kali Linux, декомпилятор Ghidra, Clang Static Analyzer, Cppcheck, OSS-Fuzz, Libfuzzer, SQLMap, NMap, OpenSSH, Eclipse, gdb, OpenJDK, dotnet, strace.

3) Программно-аппаратные ключи «РуТокен».

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима лекционная аудитория с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом.

Для проведения лабораторных занятий необходим компьютерный класс, оснащенный персональными компьютерами и необходимым программно-аппаратным обеспечением.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность и специализации «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Ассистент кафедры теоретических основ компьютерной безопасности и криптографии, заведующий учебной лабораторией компьютерной безопасности

А. А. Лобов

Программа одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «15» июня 2023 года, протокол № 14.