ГНП 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
Основы информационной безопасности

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 «Основы информационной безопасности» являются формирование базовых знаний в области обеспечения информационной безопасности, знакомство с предметной областью защиты информации, подготовка к изучению других профильных предметов.

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 «Языки программирования», «Компьютерные сети», «Аппаратные средства вычислительной техники».

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплин «Защита в операционных системах», «Основы построения защищенных компьютерных сетей», «Основы построения защищенных баз данных», «Защита программ и данных», «Программно-аппаратные средства обеспечения информационной безопасности».

Компетенции, сформированные при изучении данной дисциплины, могут быть полезны при изучении дисциплин «Основы компьютерной экспертизы», «Методы и средства криптографической защиты информации», «Защита информации от утечки по техническим каналам», «Введение в криптоанализ».

3. Результаты бучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора (индикаторов) достижения компетенции**	**Результаты обучения**
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.	ОПК-1.1.1 знает понятия информации, информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;	Знать основные положения доктрины информационной безопасности Российской федерации, принципы построения систем защиты информации; основные направления в отрасли информационной безопасности; о роли информации в современном обществе. Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, составлять модель угроз и определять их степень; подбирать способы защиты
	ОПК-1.2.1 умеет классифицировать	

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; ОПК-1.2.2 умеет анализировать профессиональные задачи, разрабатывать подходящие ИТ-решения; ОПК-1.3 владеет навыками оценивания роли информации, информационных технологий и информационной безопасности в современном обществе, их значения для обеспечения объективных потребностей личности, общества и государства.	информации Владеть навыками оценивания значимости информации.
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	ОПК-5.1.1 знает источники и классификацию угроз информационной безопасности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; ОПК-5.1.3 знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; возможности технических средств перехвата	Знать классификацию угроз информационной безопасности, основные положения доктрины информационной безопасности Российской Федерации, стратегии развития информационного общества Российской Федерации; классификацию технических каналов утечки информации, способы их эксплуатации, способы организации защиты от утечек информации по техническим каналам; основные регуляторы в области информационной безопасности. Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности, составлять модель угроз и определять их степень;

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	информации; ОПК-5.2.1 умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; ОПК-5.2.3 умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации; ОПК-5.3.1 владеет навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации.	анализировать и оценивать угрозы информационной безопасности объекта. Владеть навыками поиска специализированных документов, регламентирующих деятельность по защиты информации, и информации в них.
ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.	ОПК-11.1.1 знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков; ОПК-11.1.2 знает средства и методы хранения и передачи аутентификационной информации; основные	Знать дискреционную, мандатную и ролевую модели управления доступом, модели изолированной программной среды; о подсистемах аутентификации и аудита в операционных системах. Уметь составлять модели угроз и нарушителя безопасности. Владеть способами моделирования управления доступом и информационными потоками в компьютерных системах.

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	требования к подсистеме аудита и политике аудита; защитные механизмы и средства обеспечения безопасности операционных систем. ОПК-11.2.1 умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем; разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; ОПК-11.3.1 владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах;	

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Практические занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	6		7		8	9
1	Введение в информационную	5	1-3	6	–	–		8	Контрольная работа на 18 неделе

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Практические занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	6		7		8	9
	безопасность								
2	Задачи специалистов по защите информации		4-6	6	–	–		–	
3	Модели нарушителя и типичные атаки		7-9	6	–	–		8	
4	Информация в компьютерных системах		10-12	6	–	–		6	
5	Вредоносное программное обеспечение		13-15	6	–	–	2	6	
6	Защита информации от утечки по техническим каналам		16-18	6	–	–		6	
Промежуточная аттестация									Зачёт
	ИТОГО – 72 ч.			**36**	**–**	–	**2**	**34**	–

Содержание дисциплины

Введение в информационную безопасность. Информационная безопасность Российской Федерации. Доктрина информационной безопасности. Основные документы по информационной безопасности. Общие принципы защиты информации. Классификация угроз. Классификация данных.

Задачи специалистов по защите информации. Организация защиты информации на предприятии. Установка и настройка средств защиты информации. Анализ поступающих сигналов от средств защиты информации. Тестирование на проникновение в информационную систему. Компьютерно-техническая экспертиза. Расследование инцидентов. Исследование работы программы. Выявление уязвимостей в программах. Организация безопасной разработки программ.

Модели нарушителя и типичные атаки. Модель действий вероятного нарушителя и модель построения защиты. Классификация основных видов атак. Сетевая разведка. Средства и методы нейтрализации атак.

Информация в компьютерных системах. Конфиденциальность, целостность и доступность информации. Идентификация, аутентификация и авторизация. Парольные системы. Модели разграничения доступа. Особенности удаления информации с электронных носителей.

Вредоносное программное обеспечение. Классификация вредоносных программ. Признаки присутствия вредоносного программного обеспечения. Способы внедрения. Методы обнаружения. Методы защиты. Примеры сетевых атак. Специализированные средства и методы выявления вредоносных программ. Изолированная программная среда.

Защита информации от утечки по техническим каналам. Утечки: понятие, виды. Типовые каналы утечки информации. Технические каналы утечки. Средства и методы обнаружения технических каналов утечки информации. Средства и способы защиты от утечек по техническим каналам.

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе таких активных и интерактивных форм проведения занятий как опрос, диалог, мозговой штурм, проблемный метод, выступления экспертов и специалистов перед студентами, встречи с представителями ведущих отечественных фирм по защите информации, ознакомительные беседы с представителями потенциальных работодателей.

Иная контактная работа представляет собой индивидуальные консультации, оказываемые очно и дистанционно с использованием информационных и телекоммуникационных технологий с учётом образовательных 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. Контроль текущей успеваемости осуществляется в процессе проведения лекционных занятий.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для контрольной работы, тесты, контрольные вопросы, вопросы для проведения промежуточной аттестации (зачет). Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе дисциплины «Основы информационной безопасности».

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
5	20	0	0	30	0	10	40	100

Программа оценивания учебной деятельности студента

5 семестр

Лекции

Посещаемость, активность – от 0 до 20 баллов.

Лабораторные занятия

Не предусмотрены.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Качество выполнения заданий в рамках самостоятельной работы, грамотность оформления, глубина проработки материала – от 0 до 30 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Выполнение контрольной работы – от 0 до 10 баллов.

Промежуточная аттестация

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

При проведении промежуточной аттестации

ответ на «отлично» / «зачтено» оценивается от 31 до 40 баллов;

ответ на «хорошо» / «зачтено» оценивается от 21 до 30 баллов;

ответ на «удовлетворительно» / «зачтено» оценивается от 11 до 20 баллов;

ответ на «неудовлетворительно» / «не зачтено» оценивается от 0 до 10 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за пятый семестр по дисциплине «Основы информационной безопасности» составляет **100** баллов.

Таблица 2.1 Таблица пересчета полученной студентом суммы баллов по дисциплине «Основы информационной безопасности» в оценку (зачет)

60 баллов и более	«зачтено»
меньше 60 баллов	«не зачтено»

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1) Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510

2) Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]: учебник для вузов / О. В. Прохорова. – 3-е изд. стер. – Санкт-Петербург : Лань, 2022. - 124 с. : ил. Текст : непосредственный. URL: https://e.lanbook.com/book/185333 ISBN 978-5-8114-8924-4

3) 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: операционная система (Microsoft Windows).

2) Свободное программное обеспечение: интернет-браузер для просмотра pdf файлов, вместо Microsoft Windows можно использовать Simply Linux или другой дистрибутив на основе ядра Linux.

3) Доктрина информационной безопасности Российской Федерации (утверждена. Указом Президента РФ от 5 декабря 2016 г. № 646). URL: http://www.scrf.gov.ru/security/information/document5/ .

4) ФСТЭК России. URL: https://fstec.ru/ .

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.

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.