Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра информационных технологий и прикладной математики

ОДОБРЕНО:
Руководитель ОП
_____ С.В. Данилова
(подпись)
«_1_» _сентября_ 2023 г.

Рабочая программа дисциплины
Основы информационной безопасности

Уровень высшего образования:	бакалавриат
Квалификация выпускника:	бакалавр
Направление подготовки:	09.03.03 Прикладная информатика
Направленность (профиль) образовательной программы:	Прикладная информатика в цифровой экономике

Иваново

1. Цели освоения дисциплины

Целью дисциплины является сформировать у студентов четкое представление и понимание теоретических и прикладных знаний о современных методах обеспечения информационной безопасности в информационных инфраструктурах государственных и частнопредпринимательских предприятий и организаций.

В результате изучения дисциплины студенты должны овладеть методологическим инструментарием обеспечения информационной безопасности, методами и средствами правового, организационно-административного, физического, технического, технологического, программного, программно-аппаратного и криптографического обеспечения информационной безопасности. Изучить международные стандарты информационного обмена, определить понятия информационных угроз и особенности обеспечения информационной безопасности в условиях функционирования в России глобальных, региональных, корпоративных и локальных компьютерных сетей. Важным условием в изучении дисциплины «Основы Информационной безопасности» является изучение методов формирования электронных документов и электронного документооборота, идентификации и аутентификации пользователей и документов в информационных инфраструктурах на основе электронной цифровой подписи, а также методов управления контролем доступа, необходимых для построения защищенных информационных систем локального, регионального, корпоративного и глобального назначений. Предметом дисциплины является изложение основ правовой, организационно-административной, физической, технической, программной и программно-аппаратной защиты информации в современных информационных технологиях, средств и методов управления контролем доступа в компьютерных системах, методов идентификации и верификации пользователей и документов в открытых и специализированных современных информационных систем. Место дисциплины в области науки, техники и практики охватывает совокупность проблем, связанных с технологией и защитой информации в информационной инфраструктуре предприятий и организаций.

2. Место дисциплины в структуре ОП

Дисциплина «Основы информационной безопасности» изучается на втором курсе в 3 сем.

Дисциплина «Основы информационной безопасности» базируется на знаниях полученных студентами в процессе освоения программы по предметам: «Информационные системы, технологии и стандарты», «Правовое обеспечение профессиональной деятельности».

Для освоения данной дисциплины, обучающийся должен:

Знать: теоретические основы в области правовых основ информатики, информационных прав и свобод человека и гражданина, защиты интеллектуальных прав в информационной сфере; основы законодательства Российской Федерации в области информатики.

Уметь: применять программные средства системного, прикладного и специального назначения.

Владеть: навыками проектирования компьютерной сети (предприятия.)

Компетенции, знания, навыки и умения, полученные в ходе изучения дисциплины, должны всесторонне использоваться и развиваться студентами в дальнейшем для изучения дисциплин:

«Электронный документооборот на предприятии», «Информационные системы и технологии», «Сети и системы передачи информации».

3. Планируемые результаты обучения по дисциплине

3.1. Компетенции, формированию которых способствует дисциплина

УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;
ПК-10	Способен способность принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью
ПК-12	Способен решать задачи в области развития науки, техники и технологии с учетом нормативного правового регулирования в сфере интеллектуальной собственности

3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения формируемых компетенций

Знать: Основные понятия и определения информационной безопасности, законодательной и нормативно-правовой базы обеспечения информационной безопасности, методы и методики оценки рисков информационной безопасности, формы атак на информацию; угрозы, которым подвергается информация.

Уметь: выявлять источники, риски и формы атак на информацию, разрабатывать политику информационной безопасности компании в соответствии со стандартами безопасности, использовать криптографические модели, алгоритмы шифрования информации и аутентификации пользователей.

Владеть: знаниями для применения стандартов Государственной Технической Комиссии при Президенте Российской Федерации (Федеральная служба по техническому и экспортному контролю Российской Федерации) по проблемам

информационной безопасности в своей профессиональной деятельности,

методами и средствами защиты информации.

приобрести навыки:

- пользования библиотеками прикладных программ компьютерных систем для решения задач по защите информации в информационных технологиях
- применения стандартов Государственной Технической Комиссии при Президенте Российской Федерации (Федеральная служба по техническому и экспортному контролю Российской Федерации) по проблемам информационной безопасности в своей профессиональной деятельности;

Владеть, иметь опыт:

- определения требований и состава средств, методов и мероприятий по организации комплекса средств защиты информации в компьютерных технологиях;
- использование методов организации, планирования и контроля функционирования комплекса средств защиты информации;
- практического применения технических, программных и программно-аппаратных средств и методов защиты информации в компьютерных технологиях;
- организации системы управления контролем доступа в сетевых компьютерных технологиях и оценку их информационной безопасности

4. Объем и содержание дисциплины

Общая трудоемкость дисциплины составляет 72 ак.ч.), 2 зачетные единицы, лекции-18ч., практические-32ч. Вид аттестации – зачет.

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа

Объем иной контактной работы и самостоятельной работы обучающегося по дисциплине указан в учебном плане образовательной программы.

№ п/п	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в ак.часах, по очной/заочной форме обучения)		Формы текущего контроля успеваемости (по очной/заочной форме обучения) Формы промежуточной аттестации
			Занятия лекционного типа	Занятия семинарского типа	
1.	Введение. Понятие информационной безопасности	3	2	2	Тест
2.	Объектно-ориентированный подход информационной безопасности	3	2	2	Тест
3	Основные определения и критерии классификации угроз	3	2	2	Тест
4.	Законодательный уровень информационной безопасности	3	2	2	Тест
5.	Административный уровень информационной безопасности	3	2	2	Тест
6	Управление рисками	3	2	2	Тест
7.	Процедурный уровень информационной безопасности	3	2	2	Тест
8	Основные программно-технические меры	3		4	Тест
9	Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности	3	2	4	Тест
10	Оценочные стандарты и технические спецификации	3		4	Выступления на семинаре
11	Активный аудит	3	2	2	Тест
12	Экранирование, анализ защищенности	3		4	Тест
13	Туннелирование и управление	3		2	Тест
		Итого	18	32	Зачет

4.2. Развернутое описание содержания дисциплины по разделам (темам)

Раздел 1. Введение. Понятие информационной безопасности

Информационная безопасность рассматривается в разных контекстах(в доктрине информационной безопасности Российской Федерации , в Законе РФ "Об участии в международном информационном обмене".). Рассматриваются подходы к проблемам информационной безопасности. Спектр интересов субъектов, связанных с использованием информационных систем. Информационная безопасность на национальном, отраслевом, корпоративном или персональном уровне.

Раздел 2. О необходимости объектно-ориентированного подхода к информационной безопасности.

Вводится понятие класса, объекта, инкапсуляции, наследовании и полиморфизма. Компонентные объектные среды и их достоинства. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.

Раздел 3.Основные определения и критерии классификации угроз.

Даются понятия: атаки , злоумышленника, источника угроз. Классификация угроз. Угрозы доступности и их классификация. Основные угрозы целостности и их классификация. Угрозы конфиденциальности. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия.

Раздел 4 . Законодательный уровень информационной безопасности

Понятие и назначение Доктрины информационной безопасности. Интересы личности, общества и государства в информационной сфере. Значение информационной безопасности и ее место в системе национальной безопасности. Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации. Международные стандарты информационного обмена, правовые основы защиты государственной, коммерческой, служебной, процессуальной, профессиональной тайны и информации персонального характера. Федеральные Законы Российской Федерации по обеспечению информационной безопасности в информационных технологиях, Доктрина Информационной безопасности Российской Федерации, Концепция Национальной Безопасности Российской Федерации, нормативные и руководящие документы, Постановления Правительства Российской Федерации по проблемам обеспечения информационной безопасности, Руководящие документы и инструкции Федеральной службы по техническому и экспортному контролю (ФСТЭК) (бывшая Государственная техническая комиссия при Президенте Российской Федерации (ГТК)), Приказы и распоряжения ФСБ РФ, Ведомственные приказы и распоряжения.

Раздел 5. Административный уровень информационной безопасности

Сформулирована главная цель мер административного уровня. Дается понятие

термина "политика безопасности". Элементы политики безопасности. Политика верхнего уровня, среднего уровня. Программа безопасности организации. Управление рисками. Основные понятия. Мероприятия по управлению рисками. Подготовительные этапы управления рисками. Основные этапы управления рисками.

Раздел 6. Процедурный уровень информационной безопасности.

Основные классы мер процедурного уровня. Классы мер на процедурном уровне. Управление персоналом. Физическая защита. Методы и средства защиты информации от несанкционированного доступа. Аутенфикация пользователей по биометрическим характеристикам, клавиатурному подчерку и росписи мыши, на основе паролей и модели

«рукопожатия». Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ.

Раздел 7. Основные программно-технические меры

Основные понятия программно-технического уровня информационной безопасности Архитектурная безопасность-три принципа, содержащиеся в приведенном утверждении. Международные стандарты информационного обмена. Модели безопасности и их применение. Безопасность в сетях Internet и Intranet. Технология безопасности. Модели анализа безопасности программного обеспечения.

Раздел 8. Оценочные стандарты и технические спецификации

"Оранжевая книга" как оценочный стандарт. Шесть классов безопасности - C1, C2, B1, B2, B3, A1 и их основные характеристики. Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности. Сетевые механизмы безопасности. Администрирование средств безопасности. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".Функциональные требования. Требования доверия безопасности. Руководящие документы Гостехкомиссии России.

Раздел 9. Активный аудит

Основные понятия. Функциональные компоненты и архитектура. Шифрование. Контроль целостности. Цифровые сертификаты. Экранирование. Основные понятия. Анализ защищенности. Классификация межсетевых экранов. Анализ защищенности. Доступность. Основы мер обеспечения высокой доступности.

Раздел 10. Туннелирование и управление

Туннелирование. Управление. Основные понятия. Возможности типичных систем. Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности

5. Образовательные технологии

В качестве образовательных технологий используются предметно-ориентированные и личностно-ориентированные подходы к освоению материала :

- для каждого раздела дисциплины определены целевые установки, критерии их достижения;
- сформулированы контрольные вопросы, подготовлены тесты обучающего и контролирующего типов;
- сделан акцент на развитие инициативы и самостоятельности студентов при изучении информационных технологий;
- подготовка доклада с презентацией на теоретические темы, связанные с информационными технологиями;

Для организации самостоятельной работы студентов на сервере университета размещены электронные материалы папка МАТЕРИАЛЫ(Бреславская) (Информационная безопасность) на рабочем столе рабочих станций.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Оценка результатов освоения учебной дисциплины включает в себя: текущий контроль знаний и промежуточную аттестацию студентов, конкретные сроки и процедура проведения которых доводятся до сведения студентов в течение первых двух месяцев от начала обучения.

Текущий контроль знаний проводится в форме проведения лабораторных и практических занятий, устного итестовых заданий, выполнению контрольных работ.

Промежуточная аттестация по итогам освоения программы учебной дисциплины проводится в форме экзамена.

Условием допуска студента к экзамену является выполнение всех практических заданий лабораторных работ, и сдача отчётов по самостоятельной работе. Для оценки знаний студентов на экзамене используются тесты. Каждому студенту за отведённое время предлагается выполнить 25 тестовых заданий.

Условием положительной аттестации («отлично») является получение от 90-100 баллов правильно выполненных тестовых заданий

Студент, получает оценку «хорошо», является получение от 80-90- баллов правильно выполненных тестовых заданий

Студент, получает оценку «удовлетворительно», за работу, выполненную в не полном объеме не менее 60 правильно выполненных заданий .

Студент, получает оценку «неудовлетворительно» является получение от 59 и ниже баллов правильно выполненных тестовых заданий

В течение семестра студент обязан самостоятельно выполнять практическую работу, отчитываться на практических занятиях поэтапно о выполняемой работе.

Дисциплина разделена на ряд логически завершенных блоков (модулей), по которым проводится промежуточный контроль. Для обеспечения текущего контроля прохождения дисциплины применяется тестирующая система «Аист», которая основана на бальной оценке выполненного теста. Тестовые задания представлены в ФОС по данной дисциплине.

По окончании пятого семестра проводится экзамен. Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями, установленными в вузе. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в освоения дисциплины.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Оценка результатов освоения учебной дисциплины включает в себя: текущий контроль знаний и промежуточную аттестацию студентов, конкретные сроки и процедура проведения которых доводятся до сведения студентов в течение первых двух месяцев от начала обучения.

Текущий контроль знаний проводится в форме проведения лабораторных и практических занятий, устного итестовых заданий, выполнению контрольных работ.

Промежуточная аттестация по итогам освоения программы учебной дисциплины проводится в форме экзамена.

Условием допуска студента к экзамену является выполнение всех практических заданий лабораторных работ, и сдача отчётов по самостоятельной работе. Для оценки знаний студентов на экзамене используются тесты. Каждому студенту за отведённое время предлагается выполнить 25 тестовых заданий.

Условием положительной аттестации («отлично») является получение от 90-100 баллов правильно выполненных тестовых заданий

Студент, получает оценку «хорошо», является получение от 80-90- баллов правильно выполненных тестовых заданий

Студент, получает оценку «удовлетворительно», за работу, выполненную в не полном объеме не менее 60 правильно выполненных заданий .

Студент, получает оценку «неудовлетворительно» является получение от 59 и ниже баллов правильно выполненных тестовых заданий

В течение семестра студент обязан самостоятельно выполнять практическую работу, отчитываться на практических занятиях поэтапно о выполняемой работе.

Дисциплина разделена на ряд логически завершенных блоков (модулей), по которым проводится промежуточный контроль. Для обеспечения текущего контроля прохождения дисциплины применяется тестирующая система «Аист», которая основана на бальной оценке выполненного теста. Тестовые задания представлены в ФОС по данной дисциплине.

По окончании пятого семестра проводится экзамен. Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями, установленными в вузе. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в освоения дисциплины.

8. Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1.Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие /В.А. Сердюк; Национальный исследовательский университет –Высшая школа экономики. - Москва: Издательский дом Высшей школы экономики, 2015.-574 с.: ил. - Библиогр. в кн.-ISBN 978-5-7598-0698-1; То же [Электронный ресурс].-
URL: http://biblioclub.ru/index.php?page=book&id=440285

2.Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Управление рисками информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2013. – 130 с. URL:https://lib.fbtuit.uz/assets/files/1.-.._-..----.pdf

3.Еременко, В.Т. Управление информационной безопасностью: учебное пособие для высшего профессионального образования / В.Т. Еременко, М.Ю. Рытов, П.Н. Рязанцев, М.Н. Орешина. – Орел: ФГБОУ ВПО «Госуниверситет - УНПК», 2015. – 265 с.
URL:http://elib.oreluniver.ru/media/attach/note/2015/Eremenko_upr_inf_bezopasn.pdf?ysclid=lm9g38gee5186036703

4.Михайлов, А.В. Компьютерные вирусы и борьба с ними / А.В. Михайлов. - 4-е изд., испр. и доп.-Москва: Диалог-МИФИ, 2012. - 148 с. : ил. - ISBN 978-5-86404-236-6; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=136089 (15.03.2019).

5.Исакова А. И., Исаков М. Н. Информационные технологии: учебное пособие - Томск: Эль Контент, 2012 .http://biblioclub.ru

6.Астахов А. М.Искусство управления информационными рисками Издатель: ДМК Пресс, 2010. http://biblioclub.ru/index.php?page=book&id=86481&sr=1

7.Петренко С. А., Курбатов В. А. Политики безопасности компании при работе в Интернет Издатель: ДМК Пресс, 2011. http://biblioclub.ru/index.php?page=book&id=85101&sr=1

8. Креопалов В. В.Технические средства и методы защиты информации: учебно-практическое пособие Издатель: Евразийский открытый институт, 2011. http://biblioclub.ru/index.php?page=book&id=90753&sr=1

9. Системы и сети передачи информации - Тамбов: Издательство ФГБОУ ВПО «ТГТУ», 2012. .http://biblioclub.ru

Дополнительная литература:

1.Доктрина информационной безопасности Российской Федерации.

2.Федеральный закон Российской Федерации «Об информации, информационным технологиям и защите информации» №149-ФЗ от 27 июля 2006 года.

3. Федеральный закон от 4 июля 1996 г. «Об участие в международном информационном обмене».

4. Федеральный закон от 06 апреля 2011 г. N 63-ФЗ "Об электронной подписи".

5. Концепция национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 17 декабря 1997 г. N1300. (В редакции Указа Президента Российской Федерации от 10 января 2000 г. N24

6. Приказ ФСБ РФ №66 от 9 февраля 2005 года «Об утверждении Положения о разработке, производстве, реализации т эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)

7. Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» №351 от 17 марта 2002 года.

Программное обеспечение и Интернет-ресурсы

1. Ресурсы информационно-телекоммуникационной сети «Интернет»:
2. Система электронной поддержки образовательного процесса «Мой университет» https://uni.ivanovo.ac.ru

Профессиональные базы данных и информационно-справочные системы:

1. ЭБС «Университетская библиотека онлайн» www.biblioclub.ru; http://lib.ivanovo.ac.ru/index.php/polnotekstovye-resursy/ebs-universitetskaya-biblioteka
2. Электронная библиотека ИвГУ http://lib.ivanovo.ac.ru/index.php/polnotekstovye-resursy/elibnew
3. Электронный каталог НБ ИвГУ http://lib.ivanovo.ac.ru/index.php/ek

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

- для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения;

- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации, выполнения курсовых работ (проектов) с комплектом специализированной учебной мебели и техническими средствами обучения *(последнее выбирается при наличии курсовой работы (проекта) по дисциплине).*

Лаборатория, оснащенная лабораторным оборудованием, комплектом специализированной учебной мебели и техническими средствами обучения.

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Автор рабочей программы дисциплины: Ст.преподаватель кафедры ИТ и ПМ Бреславская И.Б.

Программа рассмотрена и утверждена на заседании кафедры Информационных технологий и прикладной математики (ИТиПМ) «01» сентября 2023 г., протокол № 1

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ Данилова С. В.
(подпись)

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ Данилова С. В.
(подпись)

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ Данилова С. В.
(подпись)