Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра информационных технологий и прикладной математики

ОДОБРЕНО:
Руководитель ОП
_____ С.В. Данилова
(подпись)
«1» 09 2021 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 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 4 сем.

Студент, приступающий к изучению дисциплины, должен обладать знаниями, умениями, навыками/опытом практической деятельности, полученными ранее в ходе изучения дисциплин: Введение в прикладную информатику, Правовые основы прикладной информатики, Охрана труда и техника безопасности, Информатика и программирование, Вычислительные машины. сети, системы и телекоммуникации.

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.)

Успешное освоение данной дисциплины будет способствовать готовности студентов к освоению дисциплин: Основы проектирования сетей и систем телекоммуникаций, Web-программирование, Корпоративные информационные системы, прохождению производственной практики, выполнению выпускной квалификационной работы.

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 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;
- законодательную и нормативно-правовую базу 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 компании в соответствии со стандартами безопасности;
- использовать криптографические модели, алгоритмы шифрования информации и аутентификации пользователей.

Иметь:

- практический опыт использования методов и средств защиты информации;
- навыки пользования библиотеками прикладных программ компьютерных систем для решения задач по защите информации в информационных технологиях;
- навыки 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;
- практический опыт определения требований и состава средств, методов и мероприятий по организации комплекса средств защиты информации в компьютерных технологиях;
- практический опыт использования методов организации, планирования и контроля функционирования комплекса средств защиты информации;
- навыки практического применения технических, программных и программно-аппаратных средств и методов защиты информации в компьютерных технологиях;
- практический опыт организации системы управления контролем доступа в сетевых компьютерных технологиях и оценку их информационной безопасности.

4. Объем и содержание дисциплины

Общая трудоемкость дисциплины составляет 144 часа, 4 зачетных единиц

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 лекцион - ного типа	Занятия семинарск ого типа	
1.	Введение. Понятие информационной безопасности	*4*	*2*	*2*	*Тест*
2.	Объектно-ориентированный подход информационной безопасности	*4*	*2*	*2*	*Тест*
3	Основные определения и критерии классификации угроз	*4*	*2*	*2*	*Тест*
4.	Законодательный уровень информационной безопасности	*4*	*2*	*2*	*Тест*
5.	Административный уровень информационной безопасности	*4*	*2*	*2*	*Тест*
6	Управление рисками	*4*	*2*	*2*	*Тест*
7.	Процедурный уровень информационной безопасности	*4*	*2*	*2*	*Тест*
8	Основные программно-технические меры	*4*		*4*	*Тест*
9	Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности	4	2	*4*	*Тест*
10	Оценочные стандарты и технические спецификации	4		*4*	*Выступления на семинаре*
11	Активный аудит	4	2	*2*	*Тест*
12	Экранирование, анализ защищенности	4		*4*	*Тест*
13	Туннелирование и управление	4		*2*	*Тест*
		Итого	18	*32*	*Экзамен*

Очно-заочная форма обучения

№ п/п	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в ак.часах, по очно-заочной форме обучения)		Формы текущего контроля успеваемости (по очно-заочной форме обучения) Формы промежуточной аттестации
			Занятия лекцион - ного типа	Занятия семинарск ого типа	
1.	Введение. Понятие информационной безопасности	*5*	*2*		*Тест*
2.	Объектно-ориентированный подход информационной безопасности	*5*	*2*		*Тест*
3	Основные определения и критерии классификации угроз	*5*	*2*	*2*	*Тест*
4.	Законодательный уровень информационной безопасности	*5*	*2*	*2*	*Тест*
5.	Административный уровень информационной безопасности	*5*	*2*		*Тест*
6	Управление рисками	*5*	*2*	*2*	*Тест*
7.	Процедурный уровень информационной безопасности	*5*	*2*	*2*	*Тест*
8	Основные программно-технические меры	*5*		*2*	*Тест*
9	Основные составляющие информационной безопасности. Важность и сложность проблемы информационной безопасности	5	2		*Тест*
10	Оценочные стандарты и технические спецификации	5		*2*	*Выступления на семинаре*
11	Активный аудит	5	2		*Тест*
12	Экранирование, анализ защищенности	5		*2*	*Тест*
13	Туннелирование и управление	5		*2*	*Тест*
		ИТОГО	18	*16*	*Экзамен*

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. В перечень информационных технологий входит также технология смешанного обучения.

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

Основная учебная литература:

1. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-238-02857-6. – Текст : электронный.

2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574729 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-7782-3640-0. – Текст : электронный.

3. Аверченков, В. И. Аудит информационной безопасности : учебное пособие : [16+] / В. И. Аверченков. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 269 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-9765-1256-6. – Текст : электронный.

4. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник : [16+] / Б. И. Филиппов, О. Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 240 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499170 (дата обращения: 01.09.2021). – Библиогр.: с. 221-226. – ISBN 978-5-4475-9823-5. – DOI 10.23681/499170. – Текст : электронный.

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.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

Система электронной поддержки образовательного процесса «Мой университет» https://uni.ivanovo.ac.ru

Облачные сервисы «Контур» https://kontur.ru/

Портал выбора ИТ поставщиков http://www.tadviser.ru/

Портал ИТ-специалистов http://habrahabr.ru/

Издательство Открытые системы http://www.osp.ru/

Профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн» www.biblioclub.ru

Электронная библиотека ИвГУ http://lib.ivanovo.ac.ru

Электронный каталог НБ ИвГУ http://lib.ivanovo.ac.ru/index.php/ek

СПС «КонсультантПлюс»

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и(или) LibreOffice, интернет-браузер Microsoft Edge и(или) Yandex Browser.

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.

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. Методические пособия презентации, краткий курс лекций практические задания располагаются на рабочем столе любой рабочей станции, находящейся в сети кафедры в папке «Материалы»/Бреславская.

Автор рабочей программы дисциплины: ст. преподаватель кафедры ИТиПМ Бреславская И.Б.

Программа рассмотрена и утверждена на заседании кафедры Информационных технологий и прикладной математики (ИТиПМ) «06» сентября 2021 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)