МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт физики

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
_____ Турилова Е.А.
"___"_____20___ г.

Программа дисциплины

Основы управления информационной безопасностью

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность телекоммуникационных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2024

Содержание

Программу дисциплины разработал(а)(и): старший преподаватель, б/с Корчагин П.А. (Кафедра радиофизики, Высшая школа киберфизических систем и прикладной электроники), Pavel.Korchagin@kpfu.ru

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ПК-1	Способен формировать цели, приоритеты, обязанности и полномочия персонала, обслуживающего защищенные телекоммуникационные системы, средства и системы их защиты от несанкционированного доступа;

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

В результате освоения дисциплины студент должен знать:

нормативные акты и стандарты в области управления информационной безопасностью.

Должен уметь:

В результате освоения дисциплины студент должен уметь: выполнять планирование, идентификацию и анализ рисков, моделировать риски, проводить мониторинг.

.

Должен владеть:

В результате освоения дисциплины студент должен владеть: специализированным программным обеспечением, пониманием структуры и системы взаимосвязи процессов управления информационной безопасностью

Должен демонстрировать способность и готовность:

К построению систему управления информационной безопасность предприятия в условиях применения современных информационных технологий.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.О.11 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность телекоммуникационных систем)" и относится к обязательной части ОПОП ВО.

Осваивается на 4 курсе в 8 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) на 108 часа(ов).

Контактная работа - 40 часа(ов), в том числе лекции - 20 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 20 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 68 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 8 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Се-местр	Виды и часы контактной работы, их трудоемкость (в часах)						Само-стоя-тель-ная ра-бота
			Лекции, всего	Лекции в эл. форме	Практи-ческие занятия, всего	Практи-ческие в эл. форме	Лабора-торные работы, всего	Лабора-торные в эл. форме	
1.	Тема 1. Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.	8	2	0	0	0	2	0	8
2.	Тема 2. Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.	8	4	0	0	0	2	0	10
3.	Тема 3. Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security.	8	4	0	0	0	2	0	10
5.	Тема 5. Современные методы и средства анализа и управление рисками информационных систем компаний.	8	2	0	0	0	4	0	8
6.	Тема 6. Правовые меры обеспечения информационной безопасности.	8	2	0	0	0	4	0	8
7.	Тема 7. Организационные меры обеспечения безопасности компьютерных информационных систем.	8	2	0	0	0	2	0	8
8.	Тема 8. Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом	8	2	0	0	0	2	0	8
10.	Тема 10. Протоколирование и аудит, шифрование, контроль целостности	8	2	0	0	0	2	0	8
	Итого		20	0	0	0	20	0	68

4.2 Содержание дисциплины (модуля)

Тема 1. Основные понятия информационной безопасности. Угрозы информационной безопасности в информационных системах.

Понятие информационной безопасности. Основные составляющие информационной безопасности. Управление информационной безопасностью. Важность и сложность проблемы информационной безопасности. Основные определения и критерии классификации угроз. Основные угрозы доступности.Основные угрозы целостности. Вредительские программы.

Тема 2. Оценочные стандарты в информационной безопасности. Стандарты управления информационной безопасностью.

Роль стандартов ИБ. Оранжевая книга как оценочный стандарт.Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.Стандарты управления информационной безопасностью

BS 7799 и ISO/IEC 17799. Их основные положения.Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". Сертификация СУИБ на соответствие ISO 27001.

Тема 3. Создание СУИБ на предприятии. Методика оценки рисков информационной безопасности компании Digital Security.

Этапы создания системы управления ИБ. Содержание этапов разработки и внедрения системы управления ИБ. Категорирование активов компании. Оценка защищенности информационной системы компании. Оценка информационных рисков. Обработка информационных рисков.Внедрение процедур системы управления ИБ. Расчет рисков по угрозе информационной безопасности. Описание архитектуры ИС. Расчет рисков по угрозе конфиденциальность.

Тема 5. Современные методы и средства анализа и управление рисками информационных систем компаний.

Обоснование необходимости инвестиций в информационную безопасность компании.Методика "Facilitated Risk Analysis Process (FRAP)". Основные этапы оценки рисков. Матрица рисков FRAP. Методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). Фазы анализа. Методика RiskWatch (риск вэтч). Критерии для оценки и управления рисками.

Тема 6. Правовые меры обеспечения информационной безопасности.

Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии. Нормативные акты предприятия по информационной безопасности. Формы правовой защиты информации на предприятии. Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности.

Тема 7. Организационные меры обеспечения безопасности компьютерных информационных систем.

Общие положения организационной защиты. Особенности организационной защиты компьютерных информационных систем и сетей. Разовые мероприятия. Периодически проводимые мероприятия. Мероприятия, проводимые по необходимости. Постоянно проводимые мероприятия. Положение о сохранности служебной информации ограниченного распространения. Приказы и распоряжения по установлению режима защиты информации. Перечень сведений, отнесенных к категории конфиденциальных. Служба безопасности предприятия.

Тема 8. Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом

Основные программно-технические меры. Программные средства защиты Превентивные, препятствующие нарушениям. Меры обнаружения нарушений. Локализующие, сужающие зону воздействия нарушений. Меры по выявлению нарушителя. Меры восстановления режима безопасности. Идентификация и аутентификация. Управление доступом.

Тема 10. Протоколирование и аудит, шифрование, контроль целостности

Протоколирование и аудит. Активный аудит. Функциональные компоненты и архитектура. Шифрование. Использование симметричного метода шифрования. Использование асимметричного метода шифрования. хэш-функция Цифровые сертификаты. Сертификат открытого ключа. Сертификат атрибутов. Классификация сертификатов.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства науки и высшего образования Российской Федерации от 6 апреля 2021 года №245)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);

- критерии оценивания сформированности компетенций;

- механизм формирования оценки по дисциплине (модулю);

- описание порядка применения и процедуры оценивания для каждого оценочного средства;

- критерии оценивания для каждого оценочного средства;

- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;

- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Интернет-портал для ИТ-специалистов - http://www.habrahabr.ru/

Интернет-портал ресурсов по информационной безопасности - http//www.all-ib.ru

Консультант Плюс - http://www.consultant.ru/

Официальный портал правовой информации - http://pravo.gov.ru/

Официальный сайт Федеральной службы по техническому и экспортному контролю - http://www.fstec.ru/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	В ходе лекционных занятий вести конспектирование учебного материала, задавая преподавателю уточняющие вопросы для разрешения спорных ситуаций. Обращать внимание содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Рекомендуется оставить в рабочих конспектах поля, на которых делать дополняющие материал пометки, подчеркивать важность тех или иных тезисов.

Вид работ	Методические рекомендации
лабораторные работы	Для подготовки к лабораторным занятиям студентам рекомендуется подробно изучить конспект лекции, предшествующей занятию и связанной с ним общей тематикой. Студент готовится по группе вопросов, выносимых на обсуждение по теме лабораторной работы. Рекомендуется проводить подготовку в небольших группах студентов (2-3 человека).
самостоя-тельная работа	В ходе самостоятельной работы студент готовится к выполнению практических заданий. Для подготовки используется материал из рекомендуемой и дополнительной литературы, а также учебно-методические пособия. Студент готовится по группе вопросов, выносимых на обсуждение по теме выполняемой лабораторной работы. Рабочая программа дисциплины в части целей, перечню знаний, умений, терминов и учебных вопросов может быть использована вами в качестве ориентира в организации обучения.
зачет	При подготовке к зачёту студент должен правильно и рационально распланировать свое время, чтобы успеть качественно и на высоком уровне подготовиться к ответам по всем вопросам. Зачёт призван побудить студента получить дополнительно новые знания. Во время подготовки к зачёту студенты также систематизируют знания, которые они приобрели при изучении разделов курса. Рекомендуемые учебники и специальная литература при изучении курса, имеются в рекомендованном списке литературы в рабочей программе по данному курсу.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки "Безопасность телекоммуникационных систем".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.О.11 Основы управления информационной безопасностью

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность телекоммуникационных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2024

Основная литература:

1. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. - 5-е изд., стер. - Санкт-Петербург : Лань, 2019. - 324 с. - ISBN 978-5-8114-4067-2. - Текст: электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/114688 (дата обращения: 19.03.2020). - Режим доступа: для авториз. пользователей.

2. Шаньгин В.Ф., Защита компьютерной информации. Эффективные методы и средства / Шаньгин В.Ф. - М. : ДМК Пресс, 2010. - 544 с. - ISBN 978-5-94074-518-1 - Текст : электронный // ЭБС 'Консультант студента' : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785940745181.html (дата обращения: 19.03.2020). - Режим доступа : по подписке.

3. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 3-е изд., перераб. и доп. - Москва : РИОР : ИНФРА-М, 2020. - 320 с. - (Высшее образование). - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1052206 (дата обращения: 19.03.2020). - Режим доступа: по подписке.

Дополнительная литература:

1. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. - Москва : ФОРУМ : ИНФРА-М, 2020. - 592 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093695 (дата обращения: 19.03.2020). - Режим доступа: по подписке.

2. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА-М, 2020. - 432 с. - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/1081318 (дата обращения: 19.03.2020). - Режим доступа: по подписке.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.О.11 Основы управления информационной безопасностью

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 10.03.01 - Информационная безопасность

Профиль подготовки: Безопасность телекоммуникационных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2024

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.