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
Проф. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Теоретические основы компьютерной безопасности

Направление подготовки: 10.04.01 - Информационная безопасность
Профиль подготовки: Информационная безопасность автоматизированных систем
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

Содержание

Программу дисциплины разработал(а)(и) младший научный сотрудник, б/с Лапшина И.Р. (НИЛ СВЧ проектирование и радиотелекоммуникации, Институт физики), IRTuktarova@kpfu.ru ; Иванов Константин Васильевич

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
ОК-2	способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения
ПК-1	способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты
ПК-15	способностью организовать выполнение работ по вводу в эксплуатацию систем и средств обеспечения информационной безопасности
ПК-2	способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности
ПК-3	способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
ПК-5	способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

-терминологию в области информационной безопасности; сущность конфиденциальности, целостности и доступности информации; модели управления доступом к

информации и обеспечения ее конфиденциальности, целостности и доступности; классификацию угроз информационной безопасности; принципы построения систем

защиты от угроз нарушения конфиденциальности, целостности и доступности информации; принципы формирования типовых политик информационной безопасности;

основы правового и организационного обеспечения информационной безопасности.

Должен уметь:

-распознавать типовые уязвимости и угрозы информационной безопасности; правильно проводить анализ уязвимостей и угроз информационной безопасности;

применять на практике основные принципы теории информационной безопасности; разрабатывать методику защиты информации, подбирать модели, методы и

средства защиты информации; применять действующую законодательную базу для решения задач защиты информации; разрабатывать проекты нормативных

документов, регламентирующих работы по защите информации.

Должен владеть:

- приемами применения и разработки моделей обеспечения конфиденциальности, управления доступом и целостностью информации в автоматизированных

информационных системах, приемами разработки моделей угроз для конкретных автоматизированных систем, приемами построения моделей защиты информационных

систем от выделенных моделей угроз;

- приемами применения готовых и разработки новых политик безопасности на основе различных применяемых для этого теоретических моделей;

- приемами проектирования систем удаленного управления безопасностью автоматизированной информационной системы

- методологией разработки нормативных документов, регламентирующих режим соблюдения государственной и коммерческой тайны на предприятии;

- нормативно-правовой базой РФ, предназначенной для регулирования обеспечения информационной безопасности объектов.

Должен демонстрировать способность и готовность:

- разрабатывать и внедрять модели обеспечения конфиденциальности, целостности и доступности информации, модели угроз, модели политик безопасности для

любого вида информационной системы на предприятиях;

- обеспечивать информационную безопасность любых типов и видов данных, хранимых, воспроизводимых и обрабатываемых в компьютерных системах любого

назначения;

- основываясь на существующем законодательстве РФ, применять и разрабатывать нормативно-правовые акты, регулирующие обеспечение информационной

безопасности на предприятии.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ОД.8 Дисциплины (модули)" основной профессиональной образовательной программы 10.04.01 "Информационная безопасность (Информационная безопасность автоматизированных систем)" и относится к обязательным дисциплинам.
Осваивается на 2 курсе в 3 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 2 зачетных(ые) единиц(ы) на 72 часа(ов).

Контактная работа - 40 часа(ов), в том числе лекции - 12 часа(ов), практические занятия - 28 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 32 часа(ов).

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

Форма промежуточного контроля дисциплины: зачет в 3 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	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Основные положения теории информационной безопасности	3	2	4	0	4
2.	Тема 2. Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз	3	2	4	0	4
3.	Тема 3. Понятие и реализация политик безопасности	3	2	6	0	6
4.	Тема 4. Управление безопасностью в компьютерной системе. Модели сетевых безопасных сред.	3	2	6	0	6

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
5.	Тема 5. Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы.	3	2	4	0	6
6.	Тема 6. Информационная безопасность в системе национальной безопасности РФ. Основы государственной политики РФ в области информационной безопасности.	3	2	4	0	6
	Итого		12	28	0	32

4.2 Содержание дисциплины (модуля)

Тема 1. Основные положения теории информационной безопасности

Информационная безопасность: основные определения. Понятие конфиденциальности, целостности, доступности информации. Формальные модели управления доступом: модель Харрисона-Руззо-Ульмана, модель Белла Ла-Падулы. Формальные модели целостности: модель Кларка-Вилсона, модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом.

Тема 2. Угрозы информационной безопасности. Теоретические основы построения систем защиты от угроз

Классификация угроз информационной безопасности. Построение систем защиты от угроз нарушения конфиденциальности информации: модель системы защиты, организационное обеспечение ИБ, идентификация и аутентификация, разграничение доступа, криптографические методы, контроль внешнего периметра, протоколирование, аудит. Построение систем защиты от угроз нарушения целостности информации: модель обеспечения целостности, криптографические методы. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем.

Тема 3. Понятие и реализация политик безопасности

Понятие политик безопасности. Понятие монитора безопасности. Описание типовых политик безопасности. Модели на основе дискретных компонент: модель АДЕПТ и модель Хартстона. Модели на основе анализа угроз системе: игровая модель и модель с полным перекрытием. Модели конечных состояний: модель Белла Ла-Падула, LWM-модель и модель Лендвера.

Тема 4. Управление безопасностью в компьютерной системе. Модели сетевых безопасных сред.

Термины и определения. Системы удаленного управления безопасности: в отсутствии локального объекта управления, при локальном объекте управления и удаленном управляющем объекте, при распределенном объекте управления. Модели воздействия внешнего злоумышленника на локальный сегмент компьютерной системы.

Тема 5. Информационное противоборство, методы и средства его ведения. Методы и средства обеспечения информационной безопасности объектов информационной сферы.

Информационное противоборство, информационная война. Методы нарушения конфиденциальности, целостности и доступности информации в условиях информационного

противоборства. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Правовые, организационно-технические и экономические методы обеспечения ИБ. Модели, стратегии и системы обеспечения информационной безопасности в условиях информационного противоборства.

Тема 6. Информационная безопасность в системе национальной безопасности РФ. Основы государственной политики РФ в области информационной безопасности.

Информационная безопасность в системе национальной безопасности РФ. Виды защищаемой информации. Роль информационной безопасности в обеспечение национальной безопасности государства. Национальные интересы РФ в информационной сфере и их обеспечение. Виды и источники угроз информационной безопасности РФ.

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 образования и науки Российской Федерации от 5 апреля 2017 года №301)

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)

International Journal of Information Security - https://link.springer.com/journal/volumesAndIssues/10207

Электронный журнал "Информационная безопасность" - http://www.itsec.ru/main.php

Электронный журнал "Хакер" - https://xakep.ru/

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

На самостоятельную работу отводится 32 академических часа. В ходе самостоятельной работы магистрант готовится к устному опросу по темам 1, 2, 5 и 6.

Для подготовки используется лекционный материал, а также материал из рекомендуемой и дополнительной литературы. Магистрант готовится по группе вопросов,

выносимых на обсуждение на практическое занятие по теме, которые предлагаются преподавателем по окончанию каждого лекционного занятия.

Устный опрос предполагает проверку усвоения магистрантами пройденного материала. Также не исключается дискуссия между магистрантом и преподавателем

по наиболее важным и спорным вопросам дисциплины с целью проверки понимания материала.

Презентации по темам 3 и 4 представляют собой развернутое решение поставленной магистрантам практической задачи по каждой из тем. В целях облегчения

ее решения преподаватель после освоения тем 3 и 4 выдает магистрантам рекомендации по подготовке к презентации.

Подготовка к зачету по осваиваемой дисциплине ведется по установленному списку вопросов, выдаваемому магистрантам преподавателем не позже чем за две недели

до даты сдачи зачета. Каждый магистрант получает на зачете билет с двумя вопросами по пройденному материалу и готовит на них письменный ответ в течение 40

минут. Сдача зачета происходит в устной форме, в случае необходимости преподаватель имеет право задавать дополнительные вопросы на любую пройденную

тему дисциплины.

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.

Компьютерный класс.

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 10.04.01 "Информационная безопасность" и магистерской программе "Информационная безопасность автоматизированных систем".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ОД.8 Теоретические основы компьютерной безопасности

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.04.01 - Информационная безопасность
Профиль подготовки: Информационная безопасность автоматизированных систем
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

Основная литература:

1. Жук А. П. Защита информации [Электронный ресурс]: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование:Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6, 500 экз. http://znanium.com/bookread.php?book=474838

2. Малюк, А.А. Теория защиты информации [Электронный ресурс] ? Электрон. дан. ? Москва : Горячая линия-Телеком, 2012. ? 184 с. ? Режим доступа: https://e.lanbook.com/book/5170

3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : учеб.-метод. пособие ? Электрон. дан. ? Москва : Горячая линия-Телеком, 2012. ? 320 с. ? Режим доступа: https://e.lanbook.com/book/5150

Дополнительная литература:

1. Основы национальной безопасности: Учебное пособие/А.И.Овчинников, А.Ю.Мамычев, А.Г.Кравченко - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 235 с.: 60x90 1/16. - (Высшее образование) (Переплёт) ISBN 978-5-369-01454-7, 300 экз.
http://znanium.com/bookread2.php?book=508513

2. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс] : учеб. пособие / А.А. Афанасьев [и др.]. ? Электрон. дан. ? Москва: Горячая линия-Телеком, 2012. ? 550 с. ? Режим доступа: https://e.lanbook.com/book/5114

3. Милославская, Н.Г. Серия 'Вопросы управление информационной безопасностью'. Выпуск 4 [Электронный ресурс] : учеб. пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. ? Электрон. дан. ? Москва : Горячая линия-Телеком, 2012. ? 214 с. ? Режим доступа: https://e.lanbook.com/book/5181

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ОД.8 Теоретические основы компьютерной безопасности

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

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Информационная безопасность автоматизированных систем

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2017

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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.