МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
проф. Таюрский Д.А.
"___"_____20___ г.

Программа дисциплины

Введение в компьютерную безопасность

Направление подготовки: 01.04.02 - Прикладная математика и информатика
Профиль подготовки: Открытая информатика
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

Содержание

Программу дисциплины разработал(а)(и) ассистент, б.с. Долгов Д.А. (кафедра системного анализа и информационных технологий, отделение фундаментальной информатики и информационных технологий), Dolgov.kfu@gmail.com

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-1	способность к абстрактному мышлению, анализу, синтезу
ОК-3	готовность к саморазвитию, самореализации, использованию творческого потенциала
ОПК-3	способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе, в новых областях знаний, непосредственно не связанных со сферой деятельности, расширять и углублять своё научное мировоззрение
ОПК-4	способностью использовать и применять углубленные знания в области прикладной математики и информатики
ПК-12	способностью к взаимодействию в рамках международных проектов и сетевых сообществ
ПК-3	способностью углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности
ПК-4	способностью разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- основные результаты теории чисел и алгебры, основные концепции информационной безопасности, понимать проблемы сложности алгоритмов

Должен уметь:

- ориентироваться в вопросах разработки надежных систем защиты информации, видах угроз информационной безопасности, оптимизации алгоритмов, используя имеющиеся знания

Должен владеть:

- теоретическими знаниями о математических основах построения криптографических алгоритмов, пользоваться OS Debian на уровне пользователя

Должен демонстрировать способность и готовность:

- применять полученные знания в своей профессиональной деятельности

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.3 Дисциплины (модули)" основной профессиональной образовательной программы 01.04.02 "Прикладная математика и информатика (Открытая информатика)" и относится к дисциплинам по выбору.
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 3 зачетных(ые) единиц(ы) на 108 часа(ов).

Контактная работа - 28 часа(ов), в том числе лекции - 14 часа(ов), практические занятия - 14 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 44 часа(ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен 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. Понятие информационной безопасности. Основные задачи информационной безопасности. Электронно-цифровая подпись с использованием алгоритма RSA.	3	2	2	0	5
2.	Тема 2. Обеспечение безопасности передачи данных в клиент-серверных приложениях.	3	2	2	0	5
3.	Тема 3. Понятие межсетевого экрана (брандмауэра). Настройка межсетевого экрана на OS Debian. Сканеры сетей.	3	2	2	0	5
4.	Тема 4. Типовая настройка безопасности в OS Debian.	3	1	1	0	5
5.	Тема 5. SQL-инъекции, XSS.Построение безопасных WEB-страниц с использованием PHP	3	2	2	0	6
6.	Тема 6. Настройки безопасности в серверах Apache, nginx.	3	1	1	0	6
7.	Тема 7. Защита информации в системах управления базами данных. Средства защиты данных в MySQL.	3	2	2	0	6
8.	Тема 8. Методы факторизации натуральных чисел и их оптимизации.	3	2	2	0	6
	Итого		14	14	0	44

4.2 Содержание дисциплины (модуля)

Тема 1. Понятие информационной безопасности. Основные задачи информационной безопасности. Электронно-цифровая подпись с использованием алгоритма RSA.

Понятие информационной безопасности, цели информационной безопасности. Обеспечение целостности электронных документов. Сетевая аутентификация, авторизация и аудит. Угрозы информационной безопасности. Современные ассиметричные стандарты шифрования. Метод RSA. Теоретико-числовые алгоритмы, лежащие в основе алгоритма RSA. Разработка электронно-цифровой подписи для электронных документов на основе алгоритма RSA.

Тема 2. Обеспечение безопасности передачи данных в клиент-серверных приложениях.

Проблемы передачи данных. Основные атаки на клиент-серверные приложения. Современные симметричные стандарты шифрования. Сеть Фейстеля. Алгоритмы DES, 3-DES. Алгоритм распределения общего ключа Диффи-Хелмана. Разработка клиент-серверного приложения с использованием алгоритмов Диффи-Хелмана и 3-DES.

Тема 3. Понятие межсетевого экрана (брандмауэра). Настройка межсетевого экрана на OS Debian. Сканеры сетей.

Стек протоколов TCP\IP и эталонная модель OSI. Протоколы передачи данных TCP, UDP. Протокол WHOIS . Сбор открытой информации с использованием протокола whois. Сканер сети nmap и примеры его использования. Межсетевой экран iptables, архитектура и принципы работы iptables. Основные цепочки iptables: input, forward, output.

Тема 4. Типовая настройка безопасности в OS Debian.

Ограничение доступа к внешним системам. Ограничение прав пользователей, групп пользователей, категории прав, установка паролей (постоянных и временных). Настройка SSH, аутентификация по криптографическим ключам, выбор способа шифрования траффика. Блокирование нежелательного трафика с помощью iptables и fail2ban.

Тема 5. SQL-инъекции, XSS.Построение безопасных WEB-страниц с использованием PHP

Основные типы web атак. SQL-инъекции, XSS атаки. Примеры SQL-инъекций, примеры XSS атак. Методы защиты от SQL-инъекций, методы защиты от XSS атак. Построение безопасных WEB-страниц с использованием языка программирования PHP. Основные функции PHP, параметры функций, примеры. Проверка вводимых данных формы.

Тема 6. Настройки безопасности в серверах Apache, nginx.

Серверное программное обеспечение. Основы веб-сервера Apache. Основные настройки конфигурационного файла кроссплатформенного веб-сервера Apache, примеры. Основы веб-сервера Nginx. Основные настройки конфигурационного файла веб-сервера Nginx, примеры. Настройки безопасности в веб-серверах Apache, nginx.

Тема 7. Защита информации в системах управления базами данных. Средства защиты данных в MySQL.

Основы реляционной системы управления базами данных MYSQL. Управление пользователями и привилегиями. Аутентификация и авторизация пользователей БД. Установка паролей, удаление анонимных пользователей. Транзакции и блокировки в MySQL. Защита файла конфигурации системы управления базами данных MySQL.

Тема 8. Методы факторизации натуральных чисел и их оптимизации.

P метод Полларда, p-1 метод Полларда. Оценка сходимости методов. Ускорение вычисления путем оптимизации операции вычисления наибольшего общего делителя (НОД) натуральных чисел. Бинарный алгоритм НОД, к-арные алгоритмы вычисления НОД. Поиск коэффициентов для обобщенного бинарного алгоритма НОД. Расширенный бинарный алгоритм НОД.

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)

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет--портал ресурсов по математическим наукам - http://www.mathnet.ru

Компьютерный форум - http://www.citforum.ru

Хабрахабр - https://habrahabr.ru/

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

Вид работ	Методические рекомендации
лекции	Работа на лекциях предполагает изучение основных теоретических концепций криптографии и информационной безопасности. Данный вид работы очень важен, так как позволяет пояснить систему профессиональной терминологии и связь между разными видами деятельности, основные алгоритмы криптографии. Лекции проводятся в дискуссионной форме, которая позволяет не только передать знания студентам, но и выслушать их мнения, убедиться в том, что студенты расставляют правильные акценты. Студентам рекомендуется активно участвовать в обсуждении, так как в этом случае они смогут высказать свои сомнения, выслушать более важную для себя аргументацию. Также важным видом деятельности на лекциях является написание конспекта. Конспект должен быть не просто записью речи преподавателя. Гораздо важнее строить конспект в виде системы тезисов, которые в краткой формы подчеркивают основные аспекты теоретического материала и проводимой дискуссии.
практические занятия	Во время практического занятия студенты должны сосредоточить внимание на ее содержании. Нужно вспомнить основные теоретические положения. Использование конспектов предлагаемого преподавателем материала поможет вспомнить основные моменты. Примеры, разобранные ранее, помогут лучше понять проблематику данный темы.
самостоя-тельная работа	Изучение предмета 'введение в компьютерную безопасность' предусматривает систематическую самостоятельную работу студентов над дополнительными материалами. Это способствует развитию навыков самоконтроля, способствующих интенсификации учебного процесса. Основная цель самостоятельной работы студентов - систематизация и активизация знаний, полученных ими на занятиях.
экзамен	Итогом предмета "введение в компьютерную безопасность" является экзамен. Во время экзамена студенты должны сосредоточить внимание на содержании билета. Нужно вспомнить основные теоретические положения. Примеры, которые ранее разбирались на занятиях, помогут лучше понять проблематику полученного задания. Пользоваться конспектом во время экзамена нельзя.

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.

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 01.04.02 "Прикладная математика и информатика" и магистерской программе "Открытая информатика".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.3 Введение в компьютерную безопасность

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 01.04.02 - Прикладная математика и информатика
Профиль подготовки: Открытая информатика
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

Основная литература:

1.Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. ISBN 978-5-8199-0331-5 - Режим доступа: http://znanium.com/catalog/product/335362

2.Малюк А.А., Введение в информационную безопасность [Электронный ресурс] : Учебное пособие для вузов / А.А. Малюк, В.С. Горбатов, В.И. Королев и др.; Под ред. В.С. Горбатова. - М. : Горячая линия - Телеком, 2011. - 288 с. - ISBN 978-5-9912-0160-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201605.html

Дополнительная литература:

1.Шаньгин В.Ф., Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785940747680.html

2.Безопасность в техносфере, 2006, №2-М.:НИЦ ИНФРА-М,2006.-64 с.[Электронный ресурс] - Режим доступа: http://znanium.com/catalog/product/431898

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.3 Введение в компьютерную безопасность

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

Направление подготовки: 01.04.02 - Прикладная математика и информатика
Профиль подготовки: Открытая информатика
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.