

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение высшего образования  
"Казанский (Приволжский) федеральный университет"  
Высшая школа информационных технологий и интеллектуальных систем



*подписано электронно-цифровой подписью*

## Программа дисциплины

Информационная безопасность

Направление подготовки: 09.03.04 - Программная инженерия

Профиль подготовки: Технологии разработки информационных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2017

## Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО
2. Место дисциплины (модуля) в структуре ОПОП ВО
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
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)
  - 4.2. Содержание дисциплины (модуля)
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
6. Фонд оценочных средств по дисциплине (модулю)
7. Перечень литературы, необходимой для освоения дисциплины (модуля)
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)
12. Средства адаптации преподавания дисциплины (модуля) к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья
13. Приложение №1. Фонд оценочных средств
14. Приложение №2. Перечень литературы, необходимой для освоения дисциплины (модуля)
15. Приложение №3. Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Программу дисциплины разработал(а)(и) Петрова И.Р.

### 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
ПК-1	готовность применять основные методы и инструменты разработки программного обеспечения

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- угрозы безопасности информации и уязвимости сетевого оборудования, системного и прикладного программного обеспечения;
- технологии защиты информации, применяемые при построении информационных систем, защите персональных компьютеров, серверов и мобильных устройств,
- основное содержание, средства и методы используемых на практике или используемых на практике или развиваемых направлений информационной защиты,
- основные механизмы защиты информации,
- принципы комплексирования средств и методов защиты информации.

Должен уметь:

- Разбираться в терминологии по защите информации;
- Выявлять уязвимости прикладного и системного программного обеспечения;
- Проводить настройку механизмов защиты информации, реализованных в операционных системах;
- Проектировать программное обеспечение с учётом необходимости использования в ходе разработки механизмов защиты информации.

Должен владеть:

- навыками практического выявления уязвимостей и минимизации последствий их использования;
- навыками настройки механизмов защиты информации, реализованных в операционных системах.

Должен демонстрировать способность и готовность:

- Применять программно-технические способы и средства для обеспечения информационной безопасности объекта.
- Проектировать программное обеспечение с учётом необходимости реализации механизмов защиты информации.

### 2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ОД.3 Дисциплины (модули)" основной профессиональной образовательной программы 09.03.04 "Программная инженерия (Технологии разработки информационных систем)" и относится к обязательным дисциплинам.

Осваивается на 3 курсе в 6 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 4 зачетных(ые) единиц(ы) на 144 часа(ов).

Контактная работа - 72 часа(ов), в том числе лекции - 36 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 36 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 36 часа(ов).

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

Форма промежуточного контроля дисциплины: экзамен в 6 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 вопросы защиты информации.	6	4	0	0	2
2.	Тема 2. Уязвимости, угрозы, атаки и их классификации.	6	4	0	0	4
3.	Тема 3. Теоретические основы защиты информации.	6	12	0	0	6
4.	Тема 4. Возможности сканеров уязвимостей.	6	2	0	6	5
5.	Тема 5. Механизмы защиты информации, реализованные в ОС семейства Windows и системном ПО.	6	4	0	8	5
6.	Тема 6. Механизмы защиты информации, реализованные в ОС семейства Linux.	6	2	0	8	5
7.	Тема 7. Механизмы защиты информации, реализованные в прикладном программном обеспечении (на примере средств разработки ПО: jira, svn ).	6	4	0	8	5
8.	Тема 8. Механизмы защиты информации, реализованные в активном сетевом оборудовании.	6	4	0	6	4
	Итого		36	0	36	36

**4.2 Содержание дисциплины (модуля)****Тема 1. Основные вопросы защиты информации.**

1.1. Введение в информационную безопасность. 1.2. Уровни представления информации и особенности ее защиты. 1.3. Основные термины и определения. 1.4. Реализация информационной защиты.

**Тема 2. Уязвимости, угрозы, атаки и их классификации.**

2.1. Уязвимости и их классификация. 2.2. Угрозы и их классификация 2.3. Атаки, их разновидности и методы защиты от них.

**Тема 3. Теоретические основы защиты информации.**

3.1 Механизмы подсистемы управления доступом 3.2. Механизмы криптографической подсистемы 3.3. Механизмы подсистемы регистрации и учёта событий 3.4. Механизмы подсистемы обеспечения целостности.

**Тема 4. Возможности сканеров уязвимостей.**

4.1. Определение и классификация сканеров уязвимостей. 4.2 Структура сканера уязвимостей. 4.3 Сценарии применения сканеров уязвимостей.

**Тема 5. Механизмы защиты информации, реализованные в ОС семейства Windows и системном ПО.**

5.1 Операционные системы семейства Windows и их подсистемы безопасности. 5.2 Компоненты системы безопасности. 5.3 Построение системы управления обновлениями 5.4 Реализация подсистемы антивирусной защиты сторонними средствами.

**Тема 6. Механизмы защиты информации, реализованные в ОС семейства Linux.**

6.1 Общий взгляд на архитектуру Linux 6.2. Создание новых пользователей в системе 6.3. Настройка подсистемы идентификации и аутентификации 6.4. Настройка подсистемы разграничения доступа к файлам 6.5. Настройка подсистемы регистрации и учёта событий 6.6 Настройки безопасности ОС семейства Linux.

**Тема 7. Механизмы защиты информации, реализованные в прикладном программном обеспечении (на примере средств разработки ПО: jira, svn ).**

7.1 Общие положения 7.2 Типы, форматы и размер данных 7.2 Особенности реализации механизмов защиты в СУБД. 7.3 Реализация средств защиты в системах контроля версий. 7.4. Реализация средств защиты информации в системах багтрекинга и проектного управления разработкой ПО.

**Тема 8. Механизмы защиты информации, реализованные в активном сетевом оборудовании.**

8.1. Компоненты корпоративной сети, определяющие уровень безопасности 8.2. Межсетевое экранирование 8.3. Обзор и классификация межсетевых экранов. 8.4. Построение системы обнаружения вторжений 8.5. Проблема эксплуатации защищённых АС, администрирование безопасности информации.

## **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

Национальный открытый университет ИНТУИТ - <http://www.intuit.ru>

Федеральная служба по техническому и экспортному контролю - <http://fstec.ru/>

Школа IT-менеджмента - <http://www.itmane.ru/mba-cso>

## **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)

Lan Agent - мониторинг компьютеров ЛС - <http://www.lanagent.ru/>

Интеллект-сервис - <http://www.it-ic.ru/>

Стандарты информационной безопасности - <http://www.arinteg.ru/articles/standarty-informatsionnoy-bezopasnosti-27697.html>

Федеральная служба по техническому и экспортному контролю - <http://fstec.ru/>

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

Вид работ	Методические рекомендации
лекции	Конспектирование лекций ведется в специально отведенной для этого тетради, каждый лист которой должен иметь поля (4-5 см) для дополнительных записей. Необходимо записывать тему и план лекций, рекомендуемую литературу к теме. Записи разделов лекции должны иметь заголовки, подзаголовки, красные строки. Для выделения разделов, выводов, определений, основных идей можно использовать цветные карандаши и фломастеры. Названные в лекции ссылки на первоисточники надо пометить на полях, чтобы при самостоятельной работе найти и вписать их. В конспекте дословно записываются определения понятий, категорий и законов. Остальное должно быть записано своими словами. Каждому студенту необходимо выработать и использовать допустимые сокращения наиболее распространенных терминов и понятий. В конспект следует заносить всё, что преподаватель пишет на доске, также рекомендуемые схемы, таблицы, диаграммы и т.д.
лабораторные работы	Главная цель лабораторных занятий - осуществить связь теоретических положений с практической действительностью, экспериментальную проверку теоретических положений. Знакомство с оборудованием и выработка навыков работы с ним, уяснение хода выполнения лабораторной работы является обязательным условием качественного выполнения работы. Кроме достижения главной цели - подтверждение теоретических положений на лабораторном занятии решаются и другие задачи. При подготовке к лабораторным работам необходимо ознакомиться с методическими указаниями той работы, которая значится в графике учебного процесса и изучить: цель работы; содержание работы; оборудование рабочего места; правила техники безопасности; общие сведения о процессах и режимах установки, стенда, порядок выполнения работы и обработку опытных данных; подготовить отчет о выполненной работе.
самостоятельная работа	В самостоятельную работу входят следующие типы работ: Подготовка к аудиторному занятию (лекция, семинар, лабораторная работа, практическое занятие) и выполнение заданий к нему. Самостоятельное прорабатывание отдельных тем предмета согласно учебно-тематическому плану. Подготовка к практике и выполнение заданий к ней. Подготовка к любым видам контрольных работ. Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.



Вид работ	Методические рекомендации
экзамен	<p>Подготовка студентов к экзамену (зачету) включает три стадии: самостоятельная работа в течение учебного года (семестра); непосредственная подготовка в дни, предшествующие экзамену (зачету); подготовка к ответу на вопросы, содержащиеся в билете.</p> <p>Подготовку к экзамену (зачету) необходимо целесообразно начать с планирования и подбора нормативно-правовых источников и литературы. Прежде всего следует внимательно перечитать учебную программу и программные вопросы для подготовки к экзамену (зачету), чтобы выделить из них наименее знакомые. Далее должен следовать этап повторения всего программного материала. На эту работу целесообразно отвести большую часть времени. Следующим этапом является самоконтроль знания изученного материала, который заключается в устных ответах на программные вопросы, выносимые на экзамен (зачет). Тезисы ответов на наиболее сложные вопросы желательно записать, так как в процессе записи включаются дополнительные моторные ресурсы памяти.</p>

### 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 09.03.04 "Программная инженерия" и профилю подготовки "Технологии разработки информационных систем".



### Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 09.03.04 - Программная инженерия

Профиль подготовки: Технологии разработки информационных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2017

#### Основная литература:

1. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие. - Казань: Казанский университет, 2012. - Режим доступа: <http://kpfu.ru/docs/F366166681/mzi.pdf> (дата обращения: 27.02.2020).
2. Баранова, Е. К. Основы информатики и защиты информации : учебное пособие / Е. К. Баранова. - Москва : РИОР : ИНФРА-М, 2013. - 183 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01169-0 (РИОР), ISBN 978-5-16-006484-0 (ИНФРА-М). - Текст : электронный. - URL: <https://znanium.com/catalog/product/415501> (дата обращения: 27.02.2020). - Режим доступа : по подписке.
3. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие/Глинская Е.В., Чичварин Н.В. - Москва : НИЦ ИНФРА-М, 2016. - 118 с. (Высшее образование: Бакалавриат) ISBN 978-5-16-010961-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/507334> (дата обращения: 27.02.2020). - Режим доступа : по подписке.

#### Дополнительная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/405000> (дата обращения: 27.02.2020). - Режим доступа : по подписке.
2. Партыка, Т. Л. Информационная безопасность: учебное пособие / Партыка Т. Л., Попов И. И. - 5-е изд., перераб. и доп. - Москва : Форум, НИЦ ИНФРА-М, 2016. - 432 с. (Профессиональное образование) ISBN 978-5-91134-627-0. - Текст : электронный. - URL: <https://znanium.com/catalog/product/516806> (дата обращения: 27.02.2020). - Режим доступа : по подписке.
3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. - Москва : ИД 'ФОРУМ' : ИНФРА-М, 2017. - 416 с. - (Профессиональное образование). - ISBN 978-5-16-101207-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/775200> (дата обращения: 27.02.2020). - Режим доступа : по подписке.

Приложение 3  
к рабочей программе дисциплины (модуля)  
Б1.В.ОД.3 Информационная безопасность

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

Направление подготовки: 09.03.04 - Программная инженерия

Профиль подготовки: Технологии разработки информационных систем

Квалификация выпускника: бакалавр

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.