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

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

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: 2020

Содержание

Программу дисциплины разработал(а)(и) Сафиуллина Л.Х.

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-10	Владение стандартами и моделями жизненного цикла

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

Терминологию в области информационной безопасности, виды и источники угроз безопасности информации, методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации; содержание основных понятий по правовому обеспечению информационной безопасности; основы безопасности операционных систем; основы безопасности вычислительных сетей; основные технические средства и методы защиты информации; основные программно-аппаратные средства обеспечения информационной безопасности.

Должен уметь:

Применять методы оценки качества и надежности программных средств; ориентироваться в системе российского и зарубежного законодательства и нормативных правовых актов, регламентирующих область ИТ; использовать правовые нормы в сфере информационной безопасности; определять актуальные источники угроз безопасности для различных профессиональных областей; выбирать методы и разрабатывать средства защиты информации.

Должен владеть:

Навыками применения современных методов сбора, обработки и анализа данных; навыками использования современных средств информационной безопасности (в т.ч. и криптографических); навыками работы с инструментальными средствами поиска уязвимости системного и прикладного программного обеспечения.

Должен демонстрировать способность и готовность:

Применять полученные знания, умения и навыки на практике.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.07 Дисциплины (модули)" основной профессиональной образовательной программы 09.03.04 "Программная инженерия (Технологии разработки информационных систем)" и относится к вариативной части.

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. Цели и задачи дисциплины					

"Информационная безопасность". Основные понятия и определения.

6	2	0	2	2

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Правовые основы защиты информации.	6	2	0	2	2
3.	Тема 3. Комплексная защита свойств информации. Системы защиты свойств конфиденциальности, целостности и доступности информации.	6	2	0	4	4
4.	Тема 4. Модели управления доступом к компьютерной системе. Дискреционная, мандатная, ролевая и атрибутивная модели.	6	2	0	2	2
5.	Тема 5. Подсистема идентификации/аутентификации.	6	2	0	2	2
6.	Тема 6. Математические основы шифрования. Симметричные алгоритмы шифрования.	6	2	0	2	2
7.	Тема 7. Блочные и поточные симметричные алгоритмы шифрования.	6	2	0	2	4
8.	Тема 8. Асимметричные алгоритмы шифрования.	6	2	0	2	2
9.	Тема 9. Методы обеспечения целостности информации.	6	2	0	2	2
10.	Тема 10. Электронная подпись. Инфраструктура открытых ключей.	6	2	0	2	2
11.	Тема 11. Методы сокрытия данных. Стеганография.	6	2	0	2	2
12.	Тема 12. Сетевые протоколы с точки зрения защиты данных.	6	2	0	2	2
13.	Тема 13. Сценарии атак на компьютерные сети и системы. Методы и технологии их отражения.	6	2	0	2	2
14.	Тема 14. Принципы защиты, лежащие в основе ОС.	6	2	0	2	2
15.	Тема 15. Технические средства ведения информационной разведки. DLP системы.	6	2	0	2	2
16.	Тема 16. Технические средства защиты и охраны.	6	2	0	2	2
17.	Тема 17. Типы вредоносного программного обеспечения. Антивирусная защита.	6	2	0	0	0
18.	Тема 18. IDS/IPS и межсетевые экраны - принципы работы, классификация, отличия.	6	2	0	2	0
	Итого		36	0	36	36

4.2 Содержание дисциплины (модуля)

Тема 1. Цели и задачи дисциплины "Информационная безопасность". Основные понятия и определения.

Цели и задачи, субъект и объект дисциплины "Инфомационная безопасность". Понятие информации в рамках дисциплины "Информационная безопасность (ИБ)" и ее свойства (конфиденциальность, целостность и доступность). Основные понятия и определения, терминология ИБ. Компьютерный инцидент. Пентест. Статистика последних лет в области ИБ.

Тема 2. Правовые основы защиты информации.

Иерархия российских нормативно-правовых актов. Доктрина информационной безопасности. Международные нормативно-правовые документы. Общие критерии безопасности информационных технологий оценки (Common Criteria), стандарты серии ISO/IEC серии 27000. PCI DSS. Федеральные законы в области ИБ. Система классификации секретной информации. Режимные помещения. Стандарты РФ в области ИБ. Организации - регуляторы в области ИБ. Сертификация средств защиты информации, средств вычислительной техники и автоматизированных систем. Аудит ИБ, модель угроз и модель нарушителя.

Тема 3. Комплексная защита свойств информации. Системы защиты свойств конфиденциальности, целостности и доступности информации.

Построение систем защиты от угроз нарушения конфиденциальности, целостности и доступности информации. Организационные меры и меры обеспечения физической безопасности. Протоколирование и аудит ИС. Принципы целостности Кларка и Вилсона. Дублирование шлюзов и межсетевых экранов. Методы резервного копирования. Использование RAID-массивов. Дублирование серверов. Кластеризация (технология SAN).

Тема 4. Модели управления доступом к компьютерной системе. Дискреционная, мандатная, ролевая и атрибутивная модели.

Классификация моделей контроля конфиденциальности и целостности информации в ИС. Формальные и неформальные модели.

Дискреционное (избирательное) управление доступом (DAC). Модель матрицы доступов Харрисона-Руззо-Ульмана. Модель Take-Grant.

Мандатное управление доступом (MAC). Модель системы безопасности Белла-ЛаПадула. Модель Low-Water-Mark. Базовое определение монитора безопасности.

Управление доступом на основе ролей (RBAC). Администрирование множества прав доступа ролей.

Управление доступом на основе атрибутов (ABAC).

Модель контроля целостности Кларка-Вилсона. Мандатная модель Кена Биба. Технологии параллельного выполнения транзакций в клиент-серверных системах.

Тема 5. Подсистема идентификации/аутентификации.

Понятия "идентификация", "аутентификация", "авторизация". Классификация способов аутентификации. Парольная аутентификацияю. Протоколы PAP, CHAP, CRAM, AAA. Проблема просмотра паролей в системе. Проблема перехвата паролей при передаче. Аутентификация на основе сертификатов. Аутентификация по одноразовым паролям. Недостатки реализации аутентификации по паролю. Использование аутентифицирующих устройств. Биометрические методы аутентификации. Регистрация и верификация биометрических данных. FAR и FRR.

Тема 6. Математические основы шифрования. Симметричные алгоритмы шифрования.

Шифрование, дешифрование, расшифрование. Криптология, криптография и криптоанализ. Гаммирование. Криптостойкость алгоритма. Имитозащита. Синхропосылка. Требования к надежным шифрсистемам. Классификация криптографических алгоритмов. Общая схема передачи ключей. Схема симметричного шифрования. Шифрование методом замены. Система шифрования Вернама. Шифрование методом перестановки. Шифрование с использованием аналитических преобразований.

Тема 7. Блочные и поточные симметричные алгоритмы шифрования.

Гаммирование (шифрование с помощью датчика случайных чисел). Генераторы псевдослучайных чисел - алгоритмы работы и область применения. Lucifer. Сеть Фейстеля. Алгоритм DES, ГОСТ 28147-89 - описание, достоинства и недостатки. Алгоритм Triple DES. Режимы работы алгоритмов: электронная кодовая книга, сцепление блоков шифра, обратная связь по шифртексту, обратная связь по выходу. Алгоритм AES. Атаки на симметричные алгоритмы шифрования. Блочные шифры.

Тема 8. Асимметричные алгоритмы шифрования.

Общая схема асимметричного шифрования. Алгоритм Диффи-Хеллмана. Описание алгоритма Диффи-Хеллмана. Генерация ключей в RSA. Описание алгоритма RSA. Надежность схемы RSA. Правила выбора параметров алгоритма RSA. Квантовые компьютеры и асимметричные алгоритмы. Область применения асимметричных криптоалгоритмов.

Тема 9. Методы обеспечения целостности информации.

Понятие "целостность данных". Методы контроля целостности данных. Полная копия данных. Контрольная сумма. Хэш. ГОСТ Р 34.11-2012 "Информационная технология. Криптографическая защита информации. Функция хэширования". Хэш-функция "Стрибог". Примеры вычисления хэшей. Имитовставка (message authenticatiob code - mac). Электронная подпись.

Тема 10. Электронная подпись. Инфраструктура открытых ключей.

Общие принципы генерации электронной подписи. Простая, неквалифицированная и квалифицированная электронные подписи (ЭП). Создание и проверка ЭП. Удостоверяющий центр. Инфраструктура открытых ключей (ИОК). Алгоритм взаимодействия в ИОК. Защищенный обмен между тремя пользователями. Иерархическая ИОК. Алгоритм проверки сертификата.

Тема 11. Методы сокрытия данных. Стеганография.

Цифровые отпечатки. Стеганографические водяные знаки. Скрытая передача данных. Алгоритмы стеганографии. Потоковые и фиксированные контейнеры. Защита исключительного и авторского права, защита подлинности документов, индивидуальные отпечаток в системе электронного документооборота, неотчуждаемость информации с использованием стеганографических алгоритмов.

Тема 12. Сетевые протоколы с точки зрения защиты данных.

Протокол Kerberos. Управление доступом по схеме однократного входа с авторизацией. Организация защищенного удаленного доступа. VPN. Криптошлюзы. Proxy. Управление идентификацией и доступом. Особенности реализации средства IPSec. Протокол управления криптоключами IKE. Защита передаваемых данных с помощью потоколов AH и ESP. Защита беспроводных сетей.

Тема 13. Сценарии атак на компьютерные сети и системы. Методы и технологии их отражения.

IP-спуфинг, атака типа "man-in-the-middle", фишинг, SQL- и php-инъекции, XSS-атака, mail-bombing, DoS- и DDoS-атаки. Buffer overflops (переполнение буфера). Сниффинг. Общее описание атаки, анализ уязвимостей, эксплуатируемых при этом. Обзор способов защиты и отражения атак. Решение кейсов проведения многоуровневых атак с точки зрения злоумышленника и офицера безопасности.

Тема 14. Принципы защиты, лежащие в основе ОС.

Центр безопасности защитника Windows. Механизмы разграничения доступа. Изоляция ядра и целостность памяти. Отчет о работоспособности и производительности. Хранение учетных записей Windows. Просмотр событий безопасности.

История создания Linux. Свойства ядра Linux. Идентификаторы пользователя и группы пользователей. Механизмы SUID и SUDO. Защита сети. Система обнаружения вторжений.

Тема 15. Технические средства ведения информационной разведки. DLP системы.

Электронные методы разведки: радиотехнические, электронно-оптические методы. Методы разведки в телекоммуникационные системах.

Технические средства электронной разведки: средства радио- и радиотехнической разведки, средства съема акустической информации, автоматические дистанционные датчики для обнаружения людей и техники, средства для негласного перехвата и регистрации информации с сетей телекоммуникации, оптоэлектронные средства.

DLP-системы при построении бизнес-процессов.

Тема 16. Технические средства защиты и охраны.

Системы охранного телевидения и видеонаблюдение. Основные параметры работы систем видеонаблюдения. Типы исполнения видеокамер. Применяемые алгоритмы обработки информации. Система контроля и управления доступом (СКУД). Обзор различных типов считывателей. Системы охранной и пожарной сигнализаций. Технологии IoT при построении объектов физической защиты информации.

Тема 17. Типы вредоносного программного обеспечения. Антивирусная защита.

Вредоносное ПО. Пути проникновения вредоносного ПО. Классификация. Программные закладки, компьютерные вирусы, сетевые черви, трояны. Основные виды троянских программ. Основные деструктивные действия, выполняемые вирусами и червями. Способы скрытия вредоносного ПО. Принципы борьбы с вредоносными ПО. Антивирусное ПО: классификация по принципу работы.

Тема 18. IDS/IPS и межсетевые экраны - принципы работы, классификация, отличия.

Система обнаружения вторжений (IDS). IDS уровня сети, уровня хоста и использованием искусственного интеллекта.

Система предотвращения вторжений. Поведенческий блокиратор. Тестирование от Current Analysis.

Фильтрация трафика с использованием межсетевого экрана (МСЭ). Классификация МСЭ: управляемые коммутаторы, пакетные фильтры, шлюзы сеансового уровня, посредники прикладного уровня, инспекторы состояния.

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

LMS Moodle КНИТУ "Информационная безопасность КФУ" - https://moodle.kstu.ru/course/view.php?id=2745

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)

База данных угроз ФСТЭК - https://bdu.fstec.ru/threat

Сайт Федеральной службы по техническому и экспортному контролю - https://fstec.ru/

Сервис создания моделей угроз - http://threat-model.com/

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

Вид работ	Методические рекомендации
лекции	Методические рекомендации по изучению дисциплины Студентам необходимо ознакомиться: - с содержанием рабочей программы дисциплины (далее - РПД), - с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, - методическими разработками по данной дисциплине, имеющимся на образовательном портале и сайте кафедры, - с графиком консультаций преподавателей кафедры. Рекомендации по подготовке к лекционным занятиям (теоретический курс) Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет. Именно поэтому контроль над систематической работой студентов всегда находится в центре внимания кафедры. Студентам необходимо: 1 - перед каждой лекцией просматривать рабочую программу дисциплины, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы; 2 - на отдельные лекции приносить соответствующий материал на бумажных носителях, представленный лектором на портале или присланный на 'электронный почтовый ящик группы' (таблицы, графики, схемы). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции; 3 - перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам.
лабораторные работы	Для прохождения курса лабораторных работ студенту необходимо: - приносить с собой рекомендованную преподавателем литературу к конкретному занятию; - до очередного лабораторного занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия; - при подготовке к лабораторным занятиям следует обязательно использовать не только лекции, учебную литературу, но и нормативно-правовые акты и материалы правоприменительной практики; - теоретический материал следует соотносить с правовыми нормами, так как в них могут быть внесены изменения, дополнения, которые не всегда отражены в учебной литературе; - в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения; - в ходе проверки выполнения лабораторной работы давать конкретные, четкие ответы по существу вопросов; - на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю. Студентам, пропустившим занятия (независимо от причин), не имеющие письменного решения задач или не подготовившиеся к данному занятию, рекомендуется не позже чем в 2-недельный срок явиться на консультацию к преподавателю и отчитаться по теме, изучавшейся на занятии. Студенты, не отчитавшиеся по каждой не проработанной ими на занятиях теме к началу зачетной сессии, упускают возможность получить положенные баллы за работу в соответствующем семестре.
самостоя-тельная работа	Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы. К выполнению заданий для самостоятельной работы предъявляются следующие требования: - задания должны исполняться самостоятельно и представляться в установленный срок, - соответствовать установленным требованиям по оформлению.
экзамен	Экзамен проводится с целью определения уровня знаний по теоретическому курсу. Экзаменационный билет состоит из двух теоретических вопросов, на каждый из которых требуется дать развернутый, аргументированный ответ. Вопросы раздаются студентам в конце семестра, по окончанию лекционных занятий. Время, которое дается на подготовку по билету - 20-30 минут.

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

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.07 Информационная безопасность

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: 2020

Основная литература:

1. Ишмухаметов Ш.Т. Математические основы защиты информации: учебное пособие. - Казань: Казанский университет, 2012. - Текст : электронный. - URL: http://kpfu.ru/docs/F366166681/mzi.pdf (дата обращения: 03.03.2020). - Режим доступа: открытый.

2. Баранова, Е. К. Основы информатики и защиты информации: учебное пособие / Баранова Е.К. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 183 с. (Высшее образование: Бакалавриат) ISBN 978-5-369-01169-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/959916 (дата обращения: 03.03.2020). - Режим доступа : по подписке.

3. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е.В. Глинская, Н.В. Чичварин. - Москва : ИНФРА-М, 2018. - 118 с. - (Высшее образование: Бакалавриат). - www.dx.doi.org/10.12737/13571. - ISBN 978-5-16-102993-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/925825 (дата обращения: 03.03.2020). - 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: 03.03.2020). - 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, 2018. - 432 с. - (Среднее профессиональное образование). - ISBN 978-5-16-101302-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/915902 (дата обращения: 03.03.2020). - Режим доступа : по подписке.

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. - Москва : ИД 'ФОРУМ' : ИНФРА-М, 2018. - 416 с. - (Среднее профессиональное образование). - ISBN 978-5-16-101207-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/945331 (дата обращения: 03.03.2020). - Режим доступа : по подписке.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.07 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: 2020

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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.