УТВЕРЖДАЮ

Проректор по учебной работе

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.С.Бирюков

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2016 г.

# **Рабочая программа дисциплины**

Защита информации

Направление подготовки (специальность)

**09.03.01 Информатика и вычислительная техника**

Присваиваемая квалификация (степень)

**бакалавр**

Форма обучения

**Очная, заочная**

Год набора-2014

Челябинск 2016г.

**Рабочая программа дисциплины согласована:**

Ученым советом института информационных технологий

Протокол заседания № \_\_ от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 2016г.

Председатель Ученого совета

ИИТ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Мельников

Секретарь Ученого совета

ИИТ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.С. Ботов

**Рабочая программа дисциплины одобрена и рекомендована кафедрой** информационных технологий и экономической информатики

Протокол заседания №\_\_ от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 2016г.

Заведующий кафедрой ИТиЭИ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ю.В.Петриченко

**Рабочая программа составлена в соответствии с требованиями** ФГОС ВО по направлению подготовки (специальности) 09.03.01 Информатика и вычислительная техника, приказ Минобрнауки № 5 от 12.01.2016г.

Автор (составитель) \_\_\_\_\_\_\_\_\_\_\_\_\_ М.Ю. Косенко

**Структура рабочей программы соответствует** приказу ректора ФГБОУ ВО «ЧелГУ» от «01» сентября 2016г. № 476-1 «Об утверждении шаблонов документов»

Начальник управления

образовательной политики \_\_\_\_\_\_\_\_\_\_\_\_ С.П. Еремеева

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_ 2016г.

**Содержание**

[**1.** **Вводная часть** 4](#_Toc461200118)

[1.1. Цели и задачи освоения учебной дисциплины 4](#_Toc461200119)

[1.2. Место учебной дисциплины в структуре образовательной программы 4](#_Toc461200120)

[1.3. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы 5](#_Toc461200121)

[**2. Структура и содержание учебной дисциплины** 5](#_Toc461200122)

[2.1. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся 5](#_Toc461200123)

[2.2. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий 6](#_Toc461200124)

[2.2.1 Лекции 7](#_Toc461200125)

[2.2.2 Практические занятия 10](#_Toc461200126)

[**3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине** 10](#_Toc461200127)

[**4.Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине** 12](#_Toc461200128)

[**5.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)** 20](#_Toc461200129)

[**6.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)** 21](#_Toc461200130)

[**7. Методические указания для обучающихся по освоению дисциплины** 21](#_Toc461200131)

[**8.Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)** 23](#_Toc461200132)

[**9.Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)** 23](#_Toc461200133)

[**10. Описание наборов демонстрационного оборудования и учебно-методических пособий, обеспечивающих тематические иллюстрации занятий лекционного типа.** 24](#_Toc461200134)

# **1.** **Вводная часть**

* 1. Цели и задачи освоения учебной дисциплины

Целью преподавания дисциплины является ознакомление студентов с современными системами информационной безопасности, организационными и техническими мерами защиты информации, экономическими и правовыми принципами их функционирования, а также возможностями использования методов защиты информации в работе с информационными ресурсами в различных областях экономики и бизнеса.

Задачами изучения дисциплины являются:

1. познакомить студентов с определением, классификацией и характеристиками информационной безопасности;
2. познакомить с организационными и экономическими аспектами работы с информационными ресурсами и методами оценки эффективности их безопасности;
3. дать представление об особенностях информационной безопасности, сегментах и участниках информационного рынка, особенностях формирования безопасности информации;
4. рассмотреть основные технологические принципы безопасности мировых информационных ресурсов на основе глобальной сети Internet;
5. рассмотреть основные механизмы обеспечения безопасности ресурсов Internet.
   1. Место учебной дисциплины в структуре образовательной программы

Дисциплина относится к базовой части. Основа дисциплины состоит из базовых знаний полученных из следующих дисциплин: «Программирование»; «Операционные системы»; «Базы данных»; «Сети и телекоммуникации»; «Локальные и глобальные вычислительные сети», «Интернет-технологии».

Знания, полученные в данной дисциплине, могут быть использованы для написания выпускной квалификационной работы.

Дисциплина изучается на 4 курсе в 7,8 семестрах у студентов очной формы обучения и на 4 курсе в 7 семестре у студентов заочной формы обучения

* 1. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины обучающийся должен овладеть следующими результатами обучения по дисциплине (модулю):

|  |  |  |
| --- | --- | --- |
| Коды компетенции (по ФГОС) | Результаты освоения ОП  Содержание компетенций согласно ФГОС | Перечень планируемых результатов обучения по дисциплине |
| ОК-4 | способностью использовать основы правовых знаний в различных сферах деятельности | Знать: государственные нормативные акты регулирующие информационную безопасность, стандарты в области информационной безопасности.  Уметь: применять основные методы и средства обеспечения безопасности. |
| ОПК-4 | способностью участвовать в настройке и наладке программно-аппаратных комплексов | Знать: основные виды угроз и уязвимостей Интернет-приложений, методы атак и защиты.  Уметь: Эксплуатировать веб-уязвимости и устранять данные уязвимости. |
| ПК-5 | способностью сопрягать аппаратные и программные средства информационных и автоматизированных систем | Знать: этапы построения системы защиты информации, понятие политики безопасности.  Уметь: применять основные методы и средства обеспечения безопасности.  Владеть: навыками настройки безопасности в Windows системе. |
| ОПК-5 | способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности | Знать: понятие информационных угроз и их виды, подходы к оценке информационных рисков; основные принципы функционирования сетей и методы обеспечения их безопасности; требования к подготовке презентаций, оформлению научно-технических отчетов.  Уметь: применять методы оценки рисков информационной безопасности, применять компьютер для производства работ в области защиты информации; настраивать основные средства обеспечения сетевой безопасности; представлять результаты работы в виде статей и докладов. |

# **2. Структура и содержание учебной дисциплины**

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

Таблица 1 - Объём дисциплины по видам учебных занятий (в часах) очной и заочной формы обучения

|  |  |  |
| --- | --- | --- |
| Объём дисциплины | Всего очной формы обучения | Всего заочной формы обучения |
| Общая трудоемкость дисциплины (ЗЕ / часы) | 6/216 | 6/216 |
| Контактная работа обучающихся с преподавателем (всего) | 84 | 16 |
| Аудиторная работа по учебному плану (всего): | 84 | 16 |
| в том числе: |  |  |
| Лекции | 42 | 2 |
| Практические занятия | 42 | 6 |
| Лабораторные работы | 0 | - |
| Самостоятельная работа обучающихся (всего) | 114 | 199 |
| Контроль | 18 | 9 |
| Вид промежуточной аттестации обучающегося | зачет, экзамен | экзамен |
| Семестр обучения | 7, 8 | 7 |

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

Таблица 2 - Разделы дисциплины, виды и объем занятий очной/заочной формы обучения

| Номер раздела, темы | Наименование разделов, тем дисциплины | Семестр | Объем в часах по видам учебной работы | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Всего | Л | ПЗ | ЛР | СРО |
|  | Основы безопасности информационных технологий | 7 | 11/9 | 7/1 | 2/1 |  | 2/7 |
|  | Обеспечение безопасности информационных технологий | 7 | 25/36,5 | 5/0,5 | 10/1 |  | 10/35 |
|  | Средства защиты информации от несанкционированного доступа | 7 | 21/17,5 | 3/0,5 | 6/1 |  | 12/16 |
|  | Обеспечение безопасности компьютерных систем и сетей | 7 | 15/36 | 3/1 | 0/0 |  | 12/35 |
|  | Обеспечение безопасности веб-ресурсов. | 8/7 | 72/110 | 24/1 | 24/3 |  | 78/106 |
|  | Всего |  | 198/207 | 42/2 | 42/6 |  | 114/199 |
|  | Контроль | 8/7 | 18/9 |  |  |  |  |
|  | Итого |  | 216 |  |  |  |  |

2.2.1 Лекции

Таблица 3 - Темы лекций, их содержание, трудоемкость очной/заочной формы обучения

|  |  |  |  |
| --- | --- | --- | --- |
| № | Тема лекции | Содержание | Общее количество часов |
|  |  | **Раздел 1. Основы безопасности информационных технологий** |  |
|  | Актуальность проблемы обеспечение безопасности информационных технологий | Основные причины обострения проблемы обеспечения безопасности информационных технологий | 7/1 |
|  | Основные понятия информационной безопасности | Информация и информационные отношения. Субъекты информационных отношений, их безопасность. Цель защиты АС и циркулирующей в ней информации. |
|  | Угрозы информационной безопасности в АС | Особенности современных АС как объекта защиты. Уязвимость основных структурно-функциональных элементов распределенных АС. Угрозы безопасности информации, АС и субъектов информационных отношений. Источники угроз безопасности. Классификация угроз безопасности. Основные непреднамеренные искусственные угрозы. Основные преднамеренные искусственные угрозы. Классификация каналов проникновения в систему и утечки информации. Неформальная модель нарушителя. |
|  | Виды мер и основные принципы обеспечения информационной безопасности | Виды мер противодействия угрозам безопасности. Правовые (законодательные). Морально-этические. Технологические. Организационные. Меры физическ ой защиты. Технические. Достоинства и недостатки различных видов мер защиты. Законодательные и морально-этические меры. Организационные меры. Физические и технические средства защиты. Основные принципы построения системы защиты ресурсов АС. |
|  | Правовые основы обеспечения информационной безопасности | Государственная система защиты информации. Лицензирование. Сертификация средств защиты и аттестование объектов информатизации. Аттестация. Юридическая значимость ЭЦП. |
|  | Основные защитные механизмы, используемые в СЗИ | Основные механизмы защиты компьютерных систем. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам АС. Списки управления доступом к объекту. Списки полномочий субъектов. Атрибутные схемы. Регистрация и оперативное оповещение о событиях безопасности. Криптографические методы Защиты информации. Криптографическое закрытие хранимых и передаваемых по каналам связи данных. Контроль целостности и аутентичности данных, передаваемых по каналам связи. Контроль целостности программных и информационных ресурсов. Управление механизмами защиты. |
|  |  | **Раздел 2. Обеспечение безопасности информационных технологий** |  |
|  | Организационная структура системы обеспечения информационной безопасности | Цели создания системы обеспечения информационной безопасности. Регламентация действий пользователей и обслуживающего персонала АС. Понятие технологии обеспечения информационной безопасности. Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты. Разовые мероприятия. Периодически проводимые мероприятия. Мероприятия, проводимые по необходимости. Постоянно проводимые мероприятия. Распределение функций по ОИБ. Система организационно-распорядительных документов по организации комплексной системы защиты информации. | 5/0,5 |
|  | Обязанности конечных пользователей и ответственных за ОИБ в подразделениях | Обязанности ответственного за обеспечение безопасности информации в подразделении. Порядок работы с носителями ключевой информации. Ответственность за нарушения. |
|  | Инструкции по организации парольной и антивирусной защиты | Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты. |
|  | Определение требований к защите ресурсов | Определение требований к защищенности информации. Категорирование защищаемых ресурсов. Категорирование защищаемых ресурсов. |
|  | Основные задачи подразделения обеспечения информационной безопасности | Организационная структура, основные функции службы компьютерной безопасности. |
|  | Концепция информационной безопасности организации | Назначение и статус документа. |
|  |  | **Раздел 3. Средства защиты информации от несанкционированного доступа** |  |
|  | Назначение и возможности СЗИ НСД | Задачи, решаемые средствами защиты информации от НСД | 3/0,5 |
|  | Рекомендации по выбору средств защиты от НСД | Распределение показателей защищенности по классам АС. Требования РД Гостехкомиссии РФ к СЗИ НСД. Сертифицированные Гостехкомиссией России СЗИ НСД. |
|  | Аппаратные средства СЗИ НСД | Аппаратные средства СЗИ НСД |
|  |  | **Раздел 4. Обеспечение безопасности компьютерных систем и сетей** |  |
|  | Угрозы, уязвимости и атаки в сетях | Основные понятия. Классификация уязвимостей. Классификация атак. | 3/1 |
|  | Сетевые средства защиты | Межсетевые экраны. Средства анализа защищенности сетей. Средства обнаружения атак. Виртуальные частные сети. |
|  |  | **Раздел 5. Обеспечение безопасности веб-ресурсов.** |  |
|  | Уязвимости веб-ресурсов. | Обзор основных уязвимостей: SQL Injection: Types of SQL Injection, Different, DBMSs, Blind SQL Injection, Cross-Site Scripting (XSS) Attacks, Cross-Site Request Forgery (CSRF) Attack, Command Injection Attacks, File Injection Attacks, Session Injection Attacks, Weak authentication and session management, Security Misconfiguration, Insufficient Transport Layer Protection.  Методы эксплуатации уязвимостей и защиты от них. | 24/1 |
|  |  | Итого | 42/2 |

2.2.2 Практические занятия

Таблица 4 — Состав и объем практического занятия очной/заочной формы обучения

| Но-мер ПЗ | Номер раздела или темы | Наименование и краткое содержание занятия | Кол-во часов | Литература и/или электронный источник |
| --- | --- | --- | --- | --- |
|  | 1 | Изучение специальной терминологии, используемой в курсе «Информационная безопасность». Создание личного терминологического словаря. | 2/1 | 1-4 |
|  | 2 | Анализ способов хранения паролей на сайтах. Изучение методов хранения паролей. Поиск потенциально небезопасных сайтов. | 2/0,5 | 1-4 |
|  | 2 | Безопасность информации в корпоративных информационных системах. Внутренние угрозы. | 4/0,25 | 1-4 |
|  | 2 | Законодательство в сфере информационной безопасности. Анализ прецедентов. | 4/0,25 | 1-4 |
|  | 3 | Системы авторизации операционных систем. | 3/0,5 | 1-4 |
|  | 3 | Изучить работу шифрованной файловой системы EFS: особенности шифрования, файлов и папок, предназначение и работа агента восстановления, способы хранения ключевой информации. | 3/0,5 | 1-4 |
|  | 5 | Обнаружение, эксплуатация и предотвращение веб-уязвимостей (SQL Injection: Types of SQL Injection, Different, DBMSs, Blind SQL Injection, Cross-Site Scripting (XSS) Attacks, Cross-Site Request Forgery (CSRF) Attack, Command Injection Attacks, File Injection Attacks, Session Injection Attacks, Weak authentication and session management, Security Misconfiguration, Insufficient Transport Layer Protection). | 24/3 | 1-4 |
| \ |  | Всего: | 42/6 |  |

# **3. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

Таблица 5 — Тема, объем и литература для СРС очной/заочной формы обучения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Номер раздела или темы | Тема СРС | Коли-  чест-во часов | Литература (ссылка на номер в списке лит-ры) и/или электронный источник (ссылка на номер источника) | Формы контроля успеваемости |
| Раздел 1. | Требования к системам и средствам защиты информации от несанкционированного доступа. | 2/7 | 1-4 | Собеседование |
| Раздел 2. | Разработка модели разграничения доступа к информации. | 2/7 | 1-4 | Собеседование |
| Раздел 2 | Управление доступом в компьютерных системах. | 2/7 | 1-4 | Собеседование |
| Раздел 2 | Задачи контроля и обеспечения безопасности информации. | 2/7 | 1-4 | Практическая работа |
| Раздел 2 | Разрушающие программные воздействия и защита от них. | 2/7 | 1-4 | Практическая работа |
| Раздел 2 | Обеспечение целостности информации | 2/7 | 1-4 | Практическая работа |
| Раздел 3 | Программно-аппаратные средства шифрования | 6/8 | 1-4 | Практическая работа |
| Раздел 3 | Методы распределения и хранения ключевой и парольной информации | 6/8 | 1-4 | Собеседование |
| Раздел 4 | Обеспечение безопасности межсетевого взаимодействия | 4/7 | 1-4 | Собеседование |
| Раздел 4 | Удаленные сетевые атаки | 2/7 | 1-4 | Практическая работа |
| Раздел 4 | Технологии межсетевых экранов | 2/7 | 1-4 | Тестирование |
| Раздел 4 | Системы обнаружения атак и вторжений | 2/7 | 1-4 | Тестирование |
| Раздел 4 | Виртуальные частные сети | 2/7 | 1-4 | Тестирование |
| Раздел 5 | Обеспечение безопасности веб-ресурсов. | 78/106 | 1-4 | Практическая работа  Тестирование |
|  | Итого | 114/199 |  |  |

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

– в форме аудиофайла.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

– в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

# **4.Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине**

4.1.Перечень компетенций с указанием этапов их формирования

Таблица 6 - Фонды оценочных средств по дисциплине

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Контролируемые разделы (темы) дисциплины  (результаты по разделам) | Код контролируемой компетенции/планируемые результаты обучения | | Наименование оценочного средства |
|  | Раздел 1,2,3,4 | ОК-4 | Знать: государственные нормативные акты регулирующие информационную безопасность, стандарты в области информационной безопасности.  Уметь: применять основные методы и средства обеспечения безопасности. | Собеседование  Проверка практической работы  Тестирование |
| ОПК-5 | Знать: понятие информационных угроз и их виды, подходы к оценке информационных рисков.  Уметь: применять методы оценки рисков информационной безопасности. | Собеседование  Проверка практической работы  Тестирование |
| ОПК-5 | Уметь: применять компьютер для производства работ в области защиты информации | Собеседование  Проверка практической работы |
| ОПК-5 | Знать: основные принципы функционирования сетей и методы обеспечения их безопасности  Уметь: настраивать основные средства обеспечения сетевой безопасности. | Собеседование  Проверка практической работы  Тестирование |
| ОПК-5 | Знать: требования к подготовке презентаций, оформлению научно-технических отчетов.  Уметь: представлять результаты работы в виде статей и докладов. | Собеседование |
| ПК-5 | Знать: этапы построения системы защиты информации, понятие политики безопасности.  Уметь: применять основные методы и средства обеспечения безопасности.  Владеть: навыками настройки безопасности в Windows системе. | Собеседование  Проверка практической работы  Тестирование |
|  | Раздел 5 | ОПК-5 | Знать: понятие информационных угроз и их виды, подходы к оценке информационных рисков.  Уметь: применять методы оценки рисков информационной безопасности. | Собеседование  Проверка практической работы  Тестирование |
| ОПК-5 | Уметь: применять компьютер для производства работ в области защиты информации | Собеседование  Проверка практической работы |
| ОПК-5 | Знать: основные принципы функционирования сетей и методы обеспечения их безопасности  Уметь: настраивать основные средства обеспечения сетевой безопасности. | Собеседование  Проверка практической работы  Тестирование |
| ОПК-5 | Знать: требования к подготовке презентаций, оформлению научно-технических отчетов.  Уметь: представлять результаты работы в виде статей и докладов. | Собеседование |
| ОПК-4 | Знать: основные виды угроз и уязвимостей Интернет-приложений, методы атак и защиты.  Уметь: Эксплуатировать веб-уязвимости и устранять данные уязвимости. | Собеседование  Проверка практической работы  Тестирование |

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

4.2. Описание показателей и критериев оценивания компетенций

4. 2.1. Собеседование

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Критерии | Уровень знаний и умений | | | |
| Отлично | Хорошо | Удовлетвори-тельно | Неудовлетво-рительно |
| Владение понятийным аппаратом | Свободно владеет понятийным аппаратом, умеет использовать его при анализе информационной безопасности. | Владеет понятийным аппаратом, но при использовании его допускает неточности. | В основном знает содержание понятий, но допускает ошибки в их использовании. | Не владеет основными понятиями по предмету. |
| Владение фактическим материалом по теме | Знание и свободное владение фактическим материалом по теме. | Незначительные неточности в изложении фактического материала. | Испытывает затруднения в изложении фактического материала. | Не владеет фактическим материалом. |
| Логичность изложения материала. | Свободное владение речью, логичность и последовательность в изложении материала. | Испытывает отдельные затруднения в логичности и последовательности изложения материала. | Материал в значительной степени излагается бессистемно и с нарушением логических связей. | Отсутствие логики в изложении материала |

Отметка «отлично» ставится в том случае, если по двум из трех критериев ответ оценивается «отлично» и по одному – на «хорошо».

Отметка «хорошо» – если по двум критериям – не ниже «хорошо» и по одному «удовлетворительно».

Отметка «удовлетворительно» – если по двум критериям не ниже «удовлетворительно» и по одному – «неудовлетворительно».

Отметка «неудовлетворительно» – если по двум и более критериям «неудовлетворительно».

4.2.2. Практическая работа

В ходе обучения дисциплине обучающийся должен выполнить набор лабораторных/практических работ. Каждую практическую работу можно зачесть, если обучающийся соответствует уровням знаний и умений согласно таблице:

| Но-мер ПЗ | Наименование и краткое содержание занятия | Уровень знаний и умений |
| --- | --- | --- |
|  | Изучение специальной терминологии, используемой в курсе «Информационная безопасность». Создание личного терминологического словаря. | Обучающийся: свободно ориентируется в терминологии; способен привести примеры; свободно может ответить на дополнительные вопросы. |
|  | Анализ способов хранения паролей на сайтах. Изучение методов хранения паролей. Поиск потенциально небезопасных сайтов. | Обучающийся: свободно ориентируется в материале тематики; владеет навыками настройки безопасности; может анализировать информацию и принимать решения; свободно может ответить на дополнительные вопросы. |
|  | Безопасность информации в корпоративных информационных системах. Внутренние угрозы. |
|  | Законодательство в сфере информационной безопасности. Анализ прецедентов. |
|  | Системы авторизации операционных систем. |
|  | Изучить работу шифрованной файловой системы EFS: особенности шифрования, файлов и папок, предназначение и работа агента восстановления, способы хранения ключевой информации. |
|  | Обнаружение и эксплуатация уязвимости SQL Injection: Types of SQL Injection, Different DBMSs, Blind SQL Injection |
|  | Обнаружение и эксплуатация уязвимости Cross-Site Scripting (XSS) Attacks |
|  | Обнаружение и эксплуатация уязвимости Cross-Site Request Forgery (CSRF) Attack |
|  | Обнаружение и эксплуатация уязвимости Command Injection Attacks |
|  | Обнаружение и эксплуатация уязвимости File Injection Attacks |
|  | Обнаружение и эксплуатация уязвимости Session Injection Attacks |
|  | Обнаружение и эксплуатация уязвимости Weak authentication and session management |
|  | Обнаружение и эксплуатация уязвимости Security Misconfiguration |
|  | Обнаружение и эксплуатация уязвимости Insufficient Transport Layer Protection |

4.2.3. Вопросы для подготовки к зачету:

1. Информация и информационные отношения. Субъекты информационных отношений, их безопасность
2. Цель защиты АС и циркулирующей в ней информации
3. Угрозы информационной безопасности в АС
4. Виды мер и основные принципы обеспечения информационной безопасности
5. Правовые основы обеспечения информационной безопасности
6. Основные защитные механизмы, используемые в СЗИ
7. Организационная структура системы обеспечения информационной безопасности
8. Основные задачи подразделения обеспечения информационной безопасности.
9. Средства защиты информации от несанкционированного доступа
10. Обеспечение безопасности компьютерных систем и сетей

4.2.4. Вопросы для подготовки к зачету:

1. Обнаружение и эксплуатация уязвимости SQL Injection: Types of SQL Injection, Different DBMSs, Blind SQL Injection
2. Обнаружение и эксплуатация уязвимости Cross-Site Scripting (XSS) Attacks
3. Обнаружение и эксплуатация уязвимости Cross-Site Request Forgery (CSRF) Attack
4. Обнаружение и эксплуатация уязвимости Command Injection Attacks
5. Обнаружение и эксплуатация уязвимости File Injection Attacks
6. Обнаружение и эксплуатация уязвимости Session Injection Attacks
7. Обнаружение и эксплуатация уязвимости Weak authentication and session management
8. Обнаружение и эксплуатация уязвимости Security Misconfiguration
9. Обнаружение и эксплуатация уязвимости Insufficient Transport Layer Protection

4.2.5. Тест.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка | Неудовлетворительно | Удовлетворительно | Хорошо | Отлично |
| Набранная сумма баллов (% выполненных заданий) (мах – 100) | Менее 60 | 60-75 | 76-90 | 91-100 |
| Оценка | Незачтено | Зачтено | | |
| Набранная сумма баллов (% выполненных заданий) (мах – 100) | Менее 60 | 60-100 | | |

4.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

Требования (критериальные показатели) к уровням освоения программы дисциплины

Для получения **«зачтено»** обучающийся должен защитить все практические задания и выполнить итоговый контрольный тест как минимум на 60%. В случае не выполнения теста на предложенный минимум обучающийся устно общается с преподавателем по курсу. В таком случае обучающийся должен глубоко и полно владеть содержанием учебного материала; уметь связывать теорию с практикой, теоретические выводы подтверждать примерами, фактами, данными научных исследований

Допустимо, что студент обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности и существенные ошибки в определении понятий, формулировке положений, не привлекает для аргументации ответа основные положения исследовательских, концептуальных и нормативных документов, не умеет обосновать свои суждения; наблюдается нарушение логики изложения. Ответ отличается низким уровнем самостоятельности, не содержит собственной профессионально-личностной позиции.

**Не зачтено** может быть поставлено обучающемуся в том случае, если он не выполнил хотя бы одну практическую работу, или если он не сдал тест. В том случае, когда обучающийся устно общается с преподавателем по курсу, он может получить «не зачтено», если онимеет разрозненные, бессистемные знания: не умеет выделять главное и второстепенное; допускает ошибки в определении понятий, формулировке теоретических положений, искажает их смысл; не ориентируется в нормативно-концептуальных, программно-методических, исследовательских материалах, беспорядочно и неуверенно излагает материал; не умеет соединять теоретические положения с практикой.

Требования (критериальные показатели) к уровням освоения программы дисциплины во втором семестре изучения дисциплины

**«Отлично» (5)** – студент глубоко и полно владеет содержанием учебного материала; умеет связывать теорию с практикой, решает микроэкономические задачи, теоретические выводы подтверждает примерами, фактами, данными научных исследований; осуществляет межпредметные связи, предложения. Делает выводы логично, четко. Ясно и кратко излагает ответы на поставленные вопросы; умеет обосновывать свои суждения и профессионально-личностную позицию по излагаемому вопросу. Ответ носит самостоятельный характер.

**«Хорошо» (4)** – ответ студента соответствует указанным выше критерия, но содержание ответа имеет отдельные неточности (несущественные ошибки) в изложении теоретического и практического материала, отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой; допущенные ошибки исправляются студентом после дополнительных вопросов экзаменатора.

**«Удовлетворительно» (3)** – студент обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности и существенные ошибки в определении понятий, формулировке положений, не привлекает для аргументации ответа основные положения исследовательских, концептуальных и нормативных документов, не умеет обосновать свои суждения; наблюдается нарушение логики изложения. Ответ отличается низким уровнем самостоятельности, не содержит собственной профессионально-личностной позиции.

**«Неудовлетворительно» (2)** – студент имеет разрозненные, бессистемные знания: не умеет выделять главное и второстепенное; допускает ошибки в определении понятий, формулировке теоретических положений, искажает их смысл; не ориентируется в нормативно-концептуальных, программно-методических, исследовательских материалах, беспорядочно и неуверенно излагает материал; не умеет соединять теоретические положения с практикой; не умеет применять знания для обоснования и объяснения фактов, не устанавливает межпредметные связи.

При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене/зачете.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

– в форме аудиофайла.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

– в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, устно с использованием услуг сурдопереводчика);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, с использованием услуг ассистента, устно).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине (модулю) может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

Пример тестового задания:

1. Какое свойство компонента (ресурса) АС заключается в том, что он доступен только тем субъектам (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия?

a конфиденциальность

b целостность

c доступность

d неотказуемость

e подотчётность

f достоверность

g аутентичность

2. Какое свойство компонента (ресурса) АС предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права?

a целостность

b конфиденциальность

c доступность

d неотказуемость

e подотчётность

f достоверность

g аутентичность

3. Какое свойство компонента (ресурса) АС означает, что имеющий соответствующие полномочия субъект может без особых проблем получить своевременный доступ к необходимому компоненту системы?

a доступность

b конфиденциальность

c целостность

d неотказуемость

e подотчётность

f достоверность

g аутентичность

# **5.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)**

Источники, отмеченные знаком «\*», имеются в научной библиотеке ЧелГУ на бумажных носителях, в электронном виде и в электронно-библиотечных системах (ЭБС) : «Университетская библиотека онлайн» и «ЛАНЬ» и др., к которым имеется подписка на текущий учебный год.

Основная литература:

1. \*Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. – Москва : Берлин : Директ-Медиа, 2015. – 253 с. – URL: <http://biblioclub.ru/index.php?page=book&id=276557> (дата обращения 26.04.2016).
2. \*Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / М.А. Иванов, И.В. Чугунков ; под ред. М.А. Иванов ; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ». – Москва : МИФИ, 2012. – 400 с. – URL: <http://biblioclub.ru/index.php?page=book&id=231673> (дата обращения 26.04.2016).
3. \*Скрипник, Д.А. Общие вопросы технической защиты информации [Электронный ресурс] / Д.А. Скрипник. – 2–е изд., испр. – М. : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. – URL: <http://biblioclub.ru/index.php?page=book&id=429070> (дата обращения 26.04.2016).

Дополнительная литература:

1. \*Аверченков, В. И. Разработка системы технической защиты информации [Электронный ресурс] : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин. – 2–е изд., стер. – Москва : Флинта, 2011. – 187 с. – URL: <http://biblioclub.ru/index.php?page=book&id=93349> (дата обращения 26.04.2016).
2. \*Аверченков, В. И. Системы защиты информации в ведущих зарубежных странах [Электронный ресурс] : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – 3–е изд., стер. – Москва : Флинта, 2011. – 224 с. – URL: <http://biblioclub.ru/index.php?page=book&id=93351> (дата обращения 26.04.2016).
3. \*Астахова, А. В. Информационные системы в экономике и защита информации на предприятиях – участниках ВЭД [Текст] : учебное пособие для вузов / А. В. Астахова. – Санкт–Петербург: Троицкий мост, 2014. – 214 с.
4. \*Борисов, М. А. Основы программно–аппаратной защиты информации [Текст] : учебное пособие для вузов / М. А. Борисов, И. В. Заводцев, И. В. Чижов. – Изд. 2–е. – Москва: [Либроком, 2013]. – 370 с.
5. Малюк, А. А. Введение в информационную безопасность [Текст] / А.А. Малюк, В. С. Горбатов, В. И. Королев, В. М. Фомичев, А. П. Дураковский, Т. А. Кондратьева. – Горячая Линия – Телеком, 2012 г., ­290 стр.
6. \*Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 5–е изд., стер. – Москва: Академия, 2011. – 331 с.
7. \*Сергеева, Ю.С. Защита информации: Конспект лекций [Электронный ресурс] : учебное пособие / Ю.С. Сергеева. – Москва : А–Приор, 2011. – 128 с. – URL: <http://biblioclub.ru/index.php?page=book&id=72670> (дата обращения 26.04.2016).

# **6.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)**

1. Moodle [Электронный ресурс]: система управления обучением : [база данных] / Челяб. гос. ун-т. – Челябинск, [б.г.]. – Доступ из сети ЧелГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: http://eu.iit.csu.ru/login/index.php (Дата обращения: 19.05.2016).
2. Искусство управления информационной безопасностью [Электронный ресурс]. - URL <http://www.iso27000.ru/>, свободный (дата обращения 26.04.2016)
3. Энциклопедия информационной безопасности. [Электронный ресурс]. - URL <http://www.wikisec.ru/>, свободный (дата обращения 26.04.2016)

# **7. Методические указания для обучающихся по освоению дисциплины**

Успешное изучение курса «Защита информации» требует от студентов посещения лекций, активной работы на семинарах, выполнения всех учебных заданий преподавателя, ознакомления с базовыми учебниками, основной и дополнительной литературой.

Запись лекции – одна из форм активной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. Культура записи лекции – один из важнейших факторов успешного и творческого овладения знаниями по современным экономическим проблемам общества. Последующая работа над текстом лекции воскрешает в памяти ее содержание, позволяет развивать экономическое мышление. В конце лекции преподаватель оставляет время (5 минут) для того, чтобы студенты имели возможность задать уточняющие вопросы по изучаемому материалу.

Лекции имеют в основном обзорный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов, а также призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что обучающиеся приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Практическое занятие – важнейшая форма работы студентов над научной, учебной и периодической литературой. Именно на практическом занятии каждый студент имеет возможность проверить глубину усвоения учебного материала, показать знание и умение работать со средствами обеспечения безопасности. Практические занятия позволяют студенту соединить полученные теоретические знания с решением конкретных практических задач.

Основным методом обучения является самостоятельная работа студентов с учебно-методическими материалами, научной литературой. Обучающийся изучает предложенную литературу и самостоятельно выполняет часть практических заданий и готовится к сдаче зачета.

К зачету необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:

 программой дисциплины;

 перечнем знаний и умений, которыми студент должен владеть;

 контрольными мероприятиями;

 учебником, учебными пособиями по дисциплине, а также электронными ресурсами;

 примерным перечнем вопросов для самоподготовки.

После этого у обучающегося должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и семинарских занятиях позволит успешно освоить дисциплину.

В освоении дисциплины (модуля) инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету является важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

# **8.Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)**

- Стандартные средства обеспечения безопасности операционной системы Windows.

- На сайте института информационных технологий http://eu.iit.csu.ru/: контент по дисциплине «Защита информации», в котором организован форум для общения как обучающихся с преподавателем, так и между собой при обсуждении тем курса. Проводятся онлайн занятия.

- Разработанные преподавателем презентации по изучаемым темам

Для инвалидов и лиц с ограниченными возможностями здоровья освоение данной дисциплины может быть осуществлено частично с использованием дистанционных образовательных технологий.

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

Лекционная аудитория с возможностью демонстрации электронных презентаций при уровне освещения, достаточном для работы с конспектом для лекций.

Компьютерный класс, оснащенный соответствующим программным обеспечением, для практических занятий.

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием средств обучения общего и специального назначения:

– лекционная аудитория – мультимедийное оборудование, мобильный радиокласс (для студентов с нарушениями слуха); источники питания для индивидуальных технических средств;

– учебная аудитория для практических занятий (семинаров) – мультимедийное оборудование, мобильный радиокласс (для студентов с нарушениями слуха);

– учебная аудитория для самостоятельной работы – стандартные рабочие места с персональными компьютерами; рабочее место с персональным компьютером, с программой экранного доступа, программой экранного увеличения и брайлевским дисплеем для студентов с нарушениями зрения.

В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, должно быть предусмотрено соответствующее количество мест для обучающихся с учетом ограничений их здоровья.

В учебные аудитории должен быть обеспечен беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья.

Перечень специальных технических средств обучения для инвалидов и лиц с ограниченными возможностями здоровья, имеющихся в Региональном учебно-научном центре инклюзивного образования ЧелГУ:

– Тифлотехническая аудитория: тифлотехнические средства: брайлевский компьютер с дисплеем и принтером, тифлокомплекс «Читающая машина», телевизионное увеличивающее устройство, тифломагнитолы кассетные и цифровые диктофоны; специальное программное обеспечение: программа речевой навигации JAWS, речевые синтезаторы («говорящая мышь»), экранные лупы.

– Сурдотехническая аудитория: радиокласс “Сонет-Р”, программируемые слуховые аппараты индивидуального пользования с устройством задания режима работы на компьютере, интерактивная доска ActiveBoard с системой голосования, акустический усилитель и колонки, мультимедийный проектор, телевизор, видеомагнитофон.

**10. Описание наборов демонстрационного оборудования и учебно-методических пособий, обеспечивающих тематические иллюстрации занятий лекционного типа.**

В образовательном процессе используется следующее демонстрационное оборудование:

разработанные преподавателем презентации по изучаемым темам, находящиеся в образовательной системе MOODLE <http://eu.iit.csu.ru/login/index.php>.