|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Частное образовательное учреждение профессионального образования  «Ставропольский многопрофильный колледж» | | | | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | УТВЕРЖДАЮ | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  | Директор | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_Н.В. Кандаурова | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| рабочая программа дисциплины | | | | | | | | | | | | | | | |
| **Управление информационной безопасностью** | | | | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Форма обучения | | **очная** | | | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Часов по учебному плану | | | 48 | |  |  |  |  |  |  | Виды контроля в семестрах: | | | |
|  |  | в том числе: | | |  |  |  |  |  |  |  | Дифференцированный зачет - 5 семестр | | |  |
|  |  | аудиторные занятия | | 48 | |  |  |  |  |  |  |  |  |  |  |
|  |  | самостоятельная работа | | 0 | |  |  |  |  |  |  |  |  |  |  |
|  |  |  | |  | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Распределение часов дисциплины по семестрам** | | | | | | | | | |  |  |  |  |  |  |
| Семестр | | | | | | **5** | | Итого | |  |  |  |  |  |  |
| Вид занятий | | | | | | УП | РПД | УП | РПД |  |  |  |  |  |  |
| Лекции | | | | | | 16 | 16 | 16 | 16 |  |  |  |  |  |  |
| Лабораторные | | | | | | 6 | 6 | 6 | 6 |  |  |  |  |  |  |
| Практические занятия | | | | | | 6 | 6 | 6 | 6 |  |  |  |  |  |  |
| Практическая подготовка | | | | | | 20 | 20 | 20 | 20 |  |  |  |  |  |  |
| Итого ауд. | | | | | | 48 | 48 | 48 | 48 |  |  |  |  |  |  |
| Контактная работа | | | | | | 48 | 48 | 48 | 48 |  |  |  |  |  |  |
| Итого | | | | | | 48 | 48 | 48 | 48 |  |  |  |  |  |  |

Программу составил(и):

преподаватель,

|  |
| --- |
| *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |

Дисциплина: **Управление информационной безопасностью**

Рабочая программа дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05Обеспечение информационной безопасности и автоматизированных систем утвержденным приказом Минобрнауки России от 09.12.2016г. № 1553.

Рабочая программа дисциплины составлена на основании учебного плана по специальности 10.02.05 Обеспечение информационной безопасности и автоматизированных систем

**Визирование РПД для исполнения в очередном учебном году**

Рабочая программа обсуждена на заседании Методического объединения укрупненной группы специальностей 09.00.00 «Информатика и вычислительная техника»; 10.00.00 «Информационная безопасность»

Протокол от 24.05.2021 № 5

Председатель МО: Харченко И.В. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рабочая программа рассмотрена и одобрена на заседании Методического совета

Протокол от 27.05.2021 № 5

Председатель МС Шляхова Н.И.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1.1 | Дисциплина «Управление информационной безопасностью» имеет своей целью формировать у обучающихся общекультурные и профессиональные компетенции в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утвержденным приказом Минобрнауки России от 09.12.2016г | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Цикл (раздел) ООП: | | | | | | ОП | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **2.1** | **Требования к предварительной подготовке обучающегося:** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **2.2** | **Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **ПК 2.1.: Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (ПК 2.1. - З - 1)  Знать: Уровень 1 | | | | | правовые основы защиты компьютерной информации | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (ПК 2.1. - З - 2)  Знать: Уровень 2 | | | | | основные методы противодействия «внутренним» угрозам информационной безопасности организации | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (ПК 2.1. - З - 3)  Знать: Уровень 3 | | | | | архитектуру основных стандартов защиты информации | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (ПК 2.1. - У - 1)  Уметь: Уровень 1 | | | | | анализировать и оценивать угрозы информационной безопасности объекта | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (ПК 2.1. - У - 2)  Уметь: Уровень 2 | | | | | применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (ПК 2.1. - У - 3)  Уметь: Уровень 3 | | | | | применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ЛР 1 | | | | | Осознающий себя гражданином и защитником великой страны | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ЛР 3 | | | | | Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ЛР 4 | | | | | Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа» | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ЛР 7 | | | | | Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности. | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **В результате освоения дисциплины обучающийся должен** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **3.1** | **Знать:** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.1.1 | правовые основы защиты компьютерной информации | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.1.2 | основные методы противодействия «внутренним» угрозам информационной безопасности организации | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.1.3 | организационные основы, принципы, методы и технологии управления подразделением службы информационной безопасности | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.1.4 | организационные, технические программные методы защиты информации в информационных системах | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.1.5 | методы идентификации пользователей | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.1.6 | архитектуру основных стандартов защиты информации | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **3.2** | **Уметь:** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.2.1 | анализировать и оценивать угрозы информационной безопасности объекта | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.2.2 | применять методы защиты компьютерной информации при проектировании информационных систем в различных предметных областях | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.2.3 | применять методы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.2.4 | выбирать необходимые методы исследования, модифицировать су-ществующие и разрабатывать новые методы, исходя из задач конкретного исследования | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.2.5 | использовать методы анализа процессов для определения актуальных угроз организации, методы оценки уровня информационной безопасности организации | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3.2.6 | анализировать информационную безопасность многопользовательских си-стем | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Код занятия** | | | **Наименование разделов и тем /вид занятия/** | | | | **Семестр / Курс** | | | | **Часов** | | | | | **Компетен-**  **ции** | | | | | **Литература** | | | | **Инте**  **ракт.** | | **Уровни сформированн ости компетенций** | | | | | |
|  | | | **Раздел 1. Управление ИБ** | | | |  | | | |  | | | | |  | | | | |  | | | |  | |  | | | | | |
| 1.1 | | | Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии. (лекция- презентация) /Лек/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 1 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(З1-3) | | | | | |
| 1.2 | | | Тема 2. Обеспечение информационной безопасности бизнеса. (лекция- презентация) /Лек/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 3 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(З1-3) | | | | | |
| 1.3 | | | Тема 3. Система управления информационной безопасностью бизнеса (лекция-презентация) /Лек/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 4 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(З1-3) | | | | | |
| 1.4 | | | Тема 4. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса (лекция-презентация) /Лек/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 7 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(З1-3) | | | | | |
| 1.5 | | | Тема 5. Социальные аспекты системы управления информационной безопасностью бизнеса (лекция- презентация) /Лек/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 1 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(З1-3) | | | | | |
| 1.6 | | | Тема 6. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации (лекция- презентация) /Лек/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 3 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(З1-3) | | | | | |
| 1.7 | | | Тема 7. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации (лекция- презентация) /Лек/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 4 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(З1-3) | | | | | |
| 1.8 | | | Тема 8. Аудит методов и средств обеспечения информационной безопасности организации (лекция- презентация) /Лек/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 7 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(З1-3) | | | | | |
| 1.9 | | | Лабораторная работа № 1. Реализация дискреционной модели политики безопасности Часть 1 /Лаб/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 1 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(У1-3) | | | | | |
| 1.10 | | | Лабораторная работа № 1. Реализация дискреционной модели политики безопасности Часть 2 /Лаб/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 3 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(У1-3) | | | | | |
| 1.11 | | | Лабораторная работа № 2. Количественная оценка стойкости парольной защиты Часть 1 /Лаб/ | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 4 | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | | | 0 | | ПК 2.1(У1-3) | | | | | |
| 1.12 | | Лабораторная работа № 2. Количественная оценка стойкости парольной защиты Часть 2 /Лаб/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 1 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.13 | | Лабораторная работа № 3. Ассиметричные алгоритмы шифрования данных Часть 1 /Лаб/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 3 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.14 | | Лабораторная работа № 3. Ассиметричные алгоритмы шифрования данных Часть 2 /Лаб/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 4 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.15 | | Лабораторная работа № 4. Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра Часть 1 /Лаб/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 7 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.16 | | Лабораторная работа № 4. Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра Часть 2 /Лаб/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 1 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.17 | | Практическое занятие 1. Организация защиты /Пр/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 3 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.18 | | Практическое занятие 2. Классификация ресурсов и их контроль /Пр/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 4 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.19 | | Практическое занятие 3. Безопасность персонала /Пр/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 7 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.20 | | Практическое занятие 4. Физическая безопасность и безопасность окружающей среды /Пр/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 1 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.21 | | Практическое занятие 5. Администрирование компьютерных систем и вычислительных сетей /Пр/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 3 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.22 | | Практическое занятие 6. Управление доступом к системам /Пр/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 4 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.23 | | Практическое занятие 7. Разработка и сопровождение информационных систем /Пр/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 7 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| 1.24 | | Практическое занятие 8. Планирование бесперебойной работы организации /Пр/ | | | | | | 5 | | | | 2 | | | | | ПК 2.1.  ЛР 1 | | | | | | | Л1.2 Л1.1 Л2.2 Л2.1 Л3.2 Л3.1  Э1 Э2 | | 0 | | ПК 2.1(У1-3) | | | | |
| **5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **5.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы:**  **Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы указан в пункте 3 настоящей рабочей программы.** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| № П/П | | Результаты обучения  (Освоенные умения, усвоенные знания) | | | | | | | | | |  | Компетенции | | | | | Формы и методы контроля и оценки результатов обучения, фонды оценочных средств | | | | | | | | | | | |  |  | |
| 1 | | ПК 2.1(З1-3) | | | | | | | | | |  | ПК 2.1. | | | | | |  | | | Вопросы к зачету по теме 1. | | | | | | | | |  | |
| 2 | | | | ПК 2.1(З1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 2. | | | | | | | | |  |
| 3 | | | | ПК 2.1(З1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 3. | | | | | | | | |  |
| 4 | | | | ПК 2.1(З1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 4. | | | | | | | | |  |
| 5 | | | | ПК 2.1(З1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 5. | | | | | | | | |  |
| 6 | | | | ПК 2.1(З1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 6. | | | | | | | | |  |
| 7 | | | | ПК 2.1(З1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 7. | | | | | | | | |  |
| 8 | | | | ПК 2.1(З1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 8. | | | | | | | | |  |
| 9 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 1. | | | | | | | | |  |
| 10 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 2. | | | | | | | | |  |
| 11 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 3. | | | | | | | | |  |
| 12 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 4. | | | | | | | | |  |
| 13 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 5. | | | | | | | | |  |
| 14 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 6. | | | | | | | | |  |
| 15 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 7. | | | | | | | | |  |
| 16 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 8. | | | | | | | | |  |
| 17 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 1. | | | | | | | | |  |
| 18 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 2. | | | | | | | | |  |
| 19 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 3. | | | | | | | | |  |
| 20 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 4. | | | | | | | | |  |
| 21 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 5. | | | | | | | | |  |
| 22 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 6. | | | | | | | | |  |
| 23 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 7. | | | | | | | | |  |
| 24 | | | | ПК 2.1(У1-3) | | | | | | | | | |  | ПК 2.1. | | | | |  | | | Вопросы к зачету по теме 8. | | | | | | | | |  |
|  | | | |  | | | | |  | | | | |  |  | | | | |  | | |  | | | | | |  | | |  |
| **5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | | |  | | | | |  | | | | |  |  | | | | |  | | |  | | | | | |  | | |  |
| Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии.  1. Деятельность по обеспечению информационной безопасности.  2. Предметная направленность деятельности по обеспечению информационной безопасности.  3. Цель деятельности по обеспечению информационной безопасности.  4. Принципы и форма деятельности по обеспечению информационной безопасности.  5. Методы деятельности по обеспечению информационной безопасности.  6. Средства обеспечения информационной безопасности.  7. Субъекты обеспечения информационной безопасности.  Тема 2. Обеспечение информационной безопасности бизнеса.  1. Информационная сущность бизнеса.  2. Роль руководства организации в обеспечении информационной безопасности.  3. Определение информационной безопасности.  4. Правовая среда бизнеса и ее свойства.  5. Внутренняя нормативная база организации.  6. Модель информационной безопасности бизнеса.  7. Обобщенная модель распределения ресурсов организации в условиях рисков.  8. Ущерб и негативные последствия.  9. Риск-ориентированный подход к обеспечению информационной безопасности бизнеса. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10. Общая модель обеспечения ИБ бизнеса.  Тема 3. Система управления информационной безопасностью бизнеса.  1. Модели непрерывного совершенствования и корпоративное управление.  2. Модели непрерывного совершенствования и международные стандарты.  3. Шаги реализации стандартной системы управления информационной безопасностью организации.  4. Модели COSO, COBIT, ITIL.  5. Контроль и аудит.  Тема 4. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса.  1. Способы оценки информационной безопасности.  2. Основные элементы процесса оценки информационной безопасности.  3. Способы измерения атрибутов объекта оценки информационной безопасности.  4. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности.  5. Модель оценки информационной безопасности на основе оценки процессов.  6. Риск-ориентированная оценка информационной безопасности.  Тема 5. Социальные аспекты системы управления информационной безопасностью бизнеса.  1. Формализованное представление угроз ИБ от персонала.  2. Общая характеристика угроз ИБ от персонала.  3. Формализованное представление угроз ИБ от персонала.  4. Противодействие угрозам ИБ от персонала.  5. Социальные аспекты угроз ИБ от персонала.  6. Личность злоумышленника.  Тема 6. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.  1. Рискообразующие факторы.  2. Структура информационного риска.  3. Понятие «Риск информационной безопасности».  4. Методика анализа риска информационной безопасности.  5. Обработка рисков информационной безопасности.  6. Процесс «Управление рисками информационной безопасности».  7. Место управления рисками информационной безопасности в структуре управления операционными рисками организации.  8. Место управления рисками информационной безопасности в структуре управления информационной безопасностью организации.  Тема 7. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.  1. Обработка рисков информационной безопасности.  2. Цели управления и средства обработки рисков информационной безопасности.  3. Модель обработки рисков информационной безопасности ISO/IEC 27001.  4. Понятие «критерий принятия риска».  5. Методы трансформации рисков информационной безопасности.  6. Анализ эффективности результатов обработки рисков.  Тема 8. Аудит методов и средств обеспечения информационной безопасности организации.  1. Аудит информационной безопасности.  2. Стандарты и практики аудита информационной безопасности.  3. Международный стандарт ISO 19011.  4. Методы организации, подготовки и проведения аудита информационной безопасности.  5. Обработка результатов аудита.  6. Место аудита информационной безопасности в структуре управления информационной безопасностью организации. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | |  | | | | | | | | | | | | | | | | | | |  | | | |
| Задания к лабораторным работам представлены в методических указаниях к практическим работам по дисциплине "Управление информационной безопасностью" для студентов специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем  Задания к практическим работам представлены в методических указаниях к практическим работам по дисциплине "Управление информационной безопасностью" для студентов специальности 10.02.05 Обеспечение информационной | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| УП: ОО10.02.05ОИБАС 2019 для РПД .osf | | | | | | | | | |  | | |  |  | |  |  | | | |  |  | | стр. 9 | |
| безопасности автоматизированных систем | | | | | | | | | | | | | | | | | | | | | | | | | |
| **5.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания** | | | | | | | | | | | | | | | | | | | | | | | | | |
| № | Наименование этапа | | | | | Компетенции | | | Технология (критерии)  оценивания компетенций | | | | Шкала (уровень) оценивания / соответствие оценке по пятибалльной шкале | | | | | | | | | | | |  |
| ниже  порогового  Ниже уровня 1 / неудовлетворите льно | пороговый  Уровень 1 / удовлетворитель но | | | Базовый  Уровень 2 / хорошо | | | | | высокий  Уровень 3/ отлично | | |  |
| 1 | Лекционные занятия | | | | | В соответсвии с п. 4 и 5.1 настоящей рабочей программы дисциплин | | | Работа  на лекциях  Участие в групповых обсуждениях | | | | отсутствие участия | единичное  высказывание | | | активное  участие в обсуждении | | | | | высказывание неординарных суждений | | |  |
| 2 | Практические и лабораторные занятия | | | | | В соответсвии с п. 4 и 5.1 настоящей рабочей программы дисциплин | | | Работа на практических занятиях  Выполнение тестов | | | | выполнение менее 50% | выполнение выше 50% | | | выполнение более 75% | | | | | выполнение более 95% | | |  |
| В соответсвии с п. 4 и 5.1 настоящей рабочей программы дисциплин | | | Работа на практических занятиях  Решение общих задач | | | | отсутствие участия в обсуждении методов решения | единичное  высказывание | | | активное  участие в обсуждении хода решения | | | | | высказывание неординарных суждений | | |  |
| 4 | Подготовка РГР, КР | | | | | В соответсвии с п. 4 и 5.1 настоящей рабочей программы дисциплин | | | Защита | | | | Не выполнение РГР, КР | защита неуверенная | | | хорошая защита | | | | | отличная защита | | |  |
| 5 | Подготовка эссе, реферата, доклада | | | | | В соответсвии с п. 4 и 5.1 настоящей рабочей программы дисциплин | | | Защита | | | | отсутствие  эссе, реферата, доклада | работа с ошибками | | | работа без ошибок с отдельными замечаниями | | | | | работа без ошибок | | |  |
| 6 | Контроль знаний  (устный или письменный ответ на экзамене, собеседование во время зачета, решение задач, выполнение иных заданий на экзамене, зачете) | | | | | В соответсвии с п. 4 и 5.1 настоящей рабочей программы дисциплин | | | Экзамен,  (Семестровый зачет) | | | | отсутствие усвоения знаний | не полное усвоение знаний | | | хорошее усвоение знаний | | | | | отличное усвоение | | |  |
| **5.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.** | | | | | | | | | | | | | | | | | | | | | | | | | |
|  |  | | |  | |  | | |  |  | | |  |  | |  |  | | | |  |  | |  |  |
| № П/П | | | | Наименование этапов формирование компетенций | | | | | | | | | | | | Компетенции | | | | | Методические материалы | | | | |
| 1 | | | | | Тема 1. Основы построения систем обеспечения информационной безопасности на предприятии. (лекция-презентация) /Лек/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 2 | | | | | Тема 2. Обеспечение информационной безопасности бизнеса. (лекция-презентация) /Лек/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 3 | | | | | Тема 3. Система управления информационной безопасностью бизнеса (лекция-презентация) /Лек/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 4 | | | | | Тема 4. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса (лекция-презентация) /Лек/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 5 | | | | | Тема 5. Социальные аспекты системы управления информационной безопасностью бизнеса (лекция-презентация) /Лек/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 6 | | | | | Тема 6. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации (лекция-презентация) /Лек/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 7 | | | | | Тема 7. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации (лекция- презентация) /Лек/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 8 | | | | | Тема 8. Аудит методов и средств обеспечения информационной безопасности организации (лекция-презентация) /Лек/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 9 | | | | | Лабораторная работа № 1. Реализация дискреционной модели политики безопасности Часть 1 /Лаб/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 10 | | | | | Лабораторная работа № 1. Реализация дискреционной модели политики безопасности Часть 2 /Лаб/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 11 | | | | | Лабораторная работа № 2. Количественная оценка стойкости парольной защиты Часть 1 /Лаб/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 12 | | | | | Лабораторная работа № 2. Количественная оценка стойкости парольной защиты Часть 2 /Лаб/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 13 | | | | | Лабораторная работа № 3. Ассиметричные алгоритмы шифрования данных Часть 1 /Лаб/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 14 | | | | | Лабораторная работа № 3. Ассиметричные алгоритмы шифрования данных Часть 2 /Лаб/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 15 | | | | | Лабораторная работа № 4. Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра Часть 1 /Лаб/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 16 | | | | | Лабораторная работа № 4. Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра Часть 2 /Лаб/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 17 | | | | | Практическое занятие 1. Организация защиты /Пр/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 18 | | | | | Практическое занятие 2. Классификация ресурсов и их контроль /Пр/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 19 | | | | | Практическое занятие 3. Безопасность персонала /Пр/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 20 | | | | | Практическое занятие 4. Физическая безопасность и безопасность окружающей среды /Пр/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 21 | | | | | Практическое занятие 5. Администрирование компьютерных систем и вычислительных сетей /Пр/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 22 | | | | | Практическое занятие 6. Управление доступом к системам /Пр/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 23 | | | | | Практическое занятие 7. Разработка и сопровождение информационных систем /Пр/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
| 24 | | | | | Практическое занятие 8. Планирование бесперебойной работы организации /Пр/ | | | | | | | | | | ПК 2.1. | | | | | Л3.1 Л3.2 | | | | | |
|  | |  | | |  | | |  | | |  | | | |  | | |  | |  | | |  | | |
| **6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)** | | | | | | | | | | | | | | | | | | | | | | | | | |
| **6.1. Рекомендуемая литература** | | | | | | | | | | | | | | | | | | | | | | | | | |
| **6.1.1. Основная литература** | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | Авторы, составители | | | | | | Заглавие | | | | | | | | | | Издательство, год | | | | | | | |
| Л1.1 | | Т.Л. Партыка, И.И. Попов | | | | | | Информационная безопасность : учеб.пособие  http://znanium.com/catalog/product/91590 | | | | | | | | | | М. : ФОРУМ : ИНФРА-М, 2018 | | | | | | | |
| **6.1.2. Дополнительная литература** | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | Авторы, составители | | | | | Заглавие | | | | | | | | | | | | Издательство, год | | | | | | |
| Л2.1 | | В.Я. Ищейнов, М.В. Мецатунян. | | | | | Основные положения информационной безопасности : учеб. Пособие  http://znanium.com/catalog/product/927190 | | | | | | | | | | | | М. : ФОРУМ : ИНФРА-М, 2018 | | | | | | |
| **6.1.3. Методические разработки, в т.ч. для самостоятельной работы** | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | Авторы, составители | | | | | Заглавие | | | | | | | | | | | | Издательство, год | | | | | | |
| Л3.1 | | Чеканов В.С. | | | | | Методические указания к практическим занятиям по дисциплине «Управление информационной безопасностью» для студентов специальности: 10.02.05 Обеспечение информационной безопасности автоматизированных систем | | | | | | | | | | | | СМК, г. Ставрополь, 2018, | | | | | | |
| Л3.2 | | Чеканов В.С. | | | | | Методические указания к лабораторным и самостоятельной работе по дисциплине «Управление информационной безопасностью» для студентов специальности: 10.02.05 Обеспечение информационной безопасности автоматизированных систем | | | | | | | | | | | | СМК, г. Ставрополь, 2018, | | | | | | |
| **6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"** | | | | | | | | | | | | | | | | | | | | | | | | | |
| Э1 | | ЭБС Знаниум | | | | | | | | | | | | | | | | | | | | | | | |
| Э2 | | Интернет Универсистет "ИНТУИТ" | | | | | | | | | | | | | | | | | | | | | | | |
| **6.3.1 Перечень программного обеспечения** | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6.3.1.1 | | | Microsoft Windows, Microsoft Office standard | | | | | | | | | | | | | | | | | | | | | | |
| **6.3.2 Перечень информационных справочных систем** | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | |  |  | | | |  | | | | |  | | | | | | |  | | | |  | | |
| **7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)** | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7.1 | | | 508. Кабинет информатики  Учебное оборудование: Стенды – 4 шт., Плакаты - 32 шт., Монитор - 16 шт., Системный блок - 16 шт., Клавиатура - 16 шт., Мышь компьютерная - 16 шт., Матрешка – Z (набор – конструктор) - 5 шт., Robobuilder RQ – HUNO (Многофункциональный робот-андроид) - 1 шт. | | | | | | | | | | | | | | | | | | | | | | |
| **8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)** | | | | | | | | | | | | | | | | | | | | | | | | | |
| Методические указания к практическим работам по дисциплине "Управление информационной безопасностью" для студентов специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем  Методические указания к лабораторным работам по дисциплине "Управление информационной безопасностью" для студентов специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем | | | | | | | | | | | | | | | | | | | | | | | | | |