МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Политехнический институт
Кафедра «Инструментальные и метрологические системы»

Утверждено на заседании кафедры
«Инструментальные и метрологические системы»
18 сентября 2024 г., протокол № 1

И.о заведующего кафедрой

_____ В.А. Белякова

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫЕ МАТЕРИАЛЫ) ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Информационная безопасность и технологии искусственного интеллекта

основной профессиональной образовательной программы высшего образования – программы бакалавриата

по направлению подготовки
27.03.04 Управление в технических системах

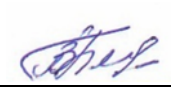
с направленностью (профилем)
Цифровые технологии в системах обеспечения качества

Форма обучения: очная

Идентификационный номер образовательной программы: 270304-01-24

Тула 2024 год

Разработчик:

Белякова В.А. к.т.н., доцент 

(ФИО, должность, ученая степень, ученое звание) *(подпись)*

1. Описание фонда оценочных средств (оценочных материалов)

Фонд оценочных средств (оценочные материалы) включает в себя контрольные задания и (или) вопросы, которые могут быть предложены обучающемуся в рамках текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю). Указанные контрольные задания и (или) вопросы позволяют оценить достижение обучающимся планируемых результатов обучения по дисциплине (модулю), установленных в соответствующей рабочей программе дисциплины (модуля), а также сформированность компетенций, установленных в соответствующей общей характеристике основной профессиональной образовательной программы.

Полные наименования компетенций и индикаторов их достижения представлены в общей характеристике основной профессиональной образовательной программы

2. Оценочные средства (оценочные материалы) для проведения текущего контроля успеваемости обучающихся по дисциплине (модулю)

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенций ОПК-5 (контролируемый индикатор достижения компетенции ОПК-5.1)

1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЕСПЕЧИВАЕТ…
1. Блокирование информации
2. Искажение информации
3. Сохранность информации
4. Утрату информации
5. Подделку информации

2. ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» БЫЛ ПРИНЯТ В СЛЕДУЮЩЕМ ГОДУ:
1. 1982
2. 1985
3. 1988
4. 1993
5. 2005

3. ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИЕЙ, ДОСТУП К КОТОРОЙ ОГРАНИЧЕН В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РФ, НАЗЫВАЕТСЯ
1. Конфиденциальная
2. Персональная
3. Документированная
4. Информация составляющая государственную тайну
5. Информация составляющая коммерческую тайну

4. ИНФОРМАЦИЯ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОПИСАНА В:
1. 1 главе Уголовного кодекса
2. 5 главе Уголовного кодекса
3. 28 главе Уголовного кодекса
4. 100 главе Уголовного кодекса
5. 1000 главе Уголовного кодекса

5. В СТАТЬЕ 272 УГОЛОВНОГО КОДЕКСА ГОВОРИТСЯ…

1. О неправомерном доступе к компьютерной информации
2. О создании, исполнении и распространении вредоносных программ для ЭВМ
3. О нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
4. О преступлениях в сфере компьютерной информации
5. Об ответственности за преступления в сфере компьютерной информации

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенций ОПК-5 (контролируемый индикатор достижения компетенции ОПК-5.2)

1. ФЕДЕРАЛЬНЫЙ ЗАКОН «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ» НАПРАВЛЕН НА:

1. Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ
2. Регулирование взаимоотношений в гражданском обществе РФ
3. Регулирование требований к работникам служб, работающих с информаций
4. Формирование необходимых норм и правил работы с информацией
5. Формирование необходимых норм и правил, связанных с защитой детей от информации

2. ХИЩЕНИЕ ИНФОРМАЦИИ – ЭТО…

1. Несанкционированное копирование информации
2. Утрата информации
3. Блокирование информации
4. Искажение информации
5. Продажа информации

3. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ПЕРВОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

1. Государство
2. Коммерческая организация
3. Муниципальное учреждение
4. Любой гражданин
5. Группа лиц, имеющих общее дело

4. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ВТОРОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

1. Простые люди
2. Государство
3. Коммерческая организация
4. Муниципальное учреждение
5. Некоммерческая организация

5. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ТРЕТЬЕЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…

1. Люди
2. Государство
3. Муниципальное учреждение
4. Учреждение
5. Некоммерческая организация

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенций ОПК-5 (контролируемый индикатор достижения компетенции ОПК-5.3)

1. ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, ВЛАДЕЮТ:

1. Государство
2. Различные учреждения
3. Государственная Дума
4. Граждане Российской Федерации
5. Медико-социальные организации

2. ПЕРСОНАЛЬНЫМИ ДАННЫМИ ВЛАДЕЮТ:
1. Государство
2. Различные учреждения
3. Государственная Дума
4. Жители Российской Федерации
5. Медико-социальные организации

3. ДОСТУП К ИНФОРМАЦИИ – ЭТО:
1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
2. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
3. Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
4. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети
5. Возможность получения информации и ее использования

4 ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТСЯ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ЭТО:
1. Конфиденциальная информация
2. Документы офера и договоров
3. Факс
4. Личный дневник
5. Законы РФ

5. ПЛАСТИКОВАЯ КАРТОЧКА, СОДЕРЖАЩАЯ ЧИП ДЛЯ КРИПТОГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ И ВСТРОЕННУЮ ЗАЩИЩЕННУЮ ПАМЯТЬ ДЛЯ ХРАНЕНИЯ ИНФОРМАЦИИ:
1. Токен
2. Password
3. Пароль
4. Login
5. Смарт-карта

3. Оценочные средства (оценочные материалы) для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенций ОПК-5 (контролируемый индикатор достижения компетенции ОПК-5.1)

1. ОСНОВНОЕ СРЕДСТВО, ОБЕСПЕЧИВАЮЩЕЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ПОСЫЛАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ, В ТОМ ЧИСЛЕ – ПО СЕТИ ИНТЕРНЕТ:

1. Идентификация
2. Аутентификация
3. Авторизация
4. Экспертиза
5. Шифрование

2. ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛАМ ИНТЕРНЕТ ИСПОЛЬЗУЕТСЯ ТЕХНОЛОГИЯ:

1. WWW
2. DICOM
3. VPN
4. FTP
5. XML

3. КОМПЛЕКС АППАРАТНЫХ И/ИЛИ ПРОГРАММНЫХ СРЕДСТВ, ОСУЩЕСТВЛЯЮЩИЙ КОНТРОЛЬ И ФИЛЬТРАЦИЮ СЕТЕВОГО ТРАФИКА В СООТВЕТСТВИИ С ЗАДАННЫМИ ПРАВИЛАМИ И ЗАЩИЩАЮЩИЙ КОМПЬЮТЕРНЫЕ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА:

1. Антивирус
2. Замок
3. Брандма́уэр
4. Криптография
5. Экспертная система

4. ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ ДАННЫЙ ВИД НАКАЗАНИЯ НА СЕГОДНЯШНИЙ ДЕНЬ НЕ ПРЕДУСМОТРЕН:

1. Дисциплинарные взыскания
2. Административный штраф
3. Уголовная ответственность
4. Лишение свободы
5. Смертная казнь

5. НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ ЭТО:

1. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
2. Работа на чужом компьютере без разрешения его владельца
3. Вход на компьютер с использованием данных другого пользователя
4. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
5. Доступ к СУБД под запрещенным именем пользователя

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенций ОПК-5 (контролируемый индикатор достижения компетенции ОПК-5.2)

1. В ДАННОМ СЛУЧАЕ СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

1. Выход в Интернет без разрешения администратора

2. При установке компьютерных игр
3. В случаях установки нелицензионного ПО
4. В случае не выхода из информационной системы
5. В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

2. МОЖЕТ ЛИ СОТРУДНИК БЫТЬ ПРИВЛЕЧЕН К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ:
1. Нет, только к административной ответственности
2. Нет, если это государственное предприятие
3. Да
4. Да, но только в случае, если действия сотрудника нанесли непоправимый вред
5. Да, но только в случае осознанных неправомочных действий сотрудника

3 ПРОЦЕДУРА, ПРОВЕРЯЮЩАЯ, ИМЕЕТ ЛИ ПОЛЬЗОВАТЕЛЬ С ПРЕДЪЯВЛЕННЫМ ИДЕНТИФИКАТОРОМ ПРАВО НА ДОСТУП К РЕСУРСУ ЭТО:
1. Идентификация
2. Аутентификация
3. Стратификация
4. Регистрация
5. Авторизация

4 НАИБОЛЕЕ ОПАСНЫМ ИСТОЧНИКОМ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ЯВЛЯЮТСЯ:
1. Другие предприятия (конкуренты)
2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
3. Рядовые сотрудники предприятия
4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
5. Хакеры

5. ВЫБЕРИТЕ, МОЖНО ЛИ В СЛУЖЕБНЫХ ЦЕЛЯХ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННЫЙ АДРЕС (ПОЧТОВЫЙ ЯЩИК), ЗАРЕГИСТРИРОВАННЫЙ НА ОБЩЕДОСТУПНОМ ПОЧТОВОМ СЕРВЕРЕ, НАПРИМЕР НА MAIL.RU:
1. Нет, не при каких обстоятельствах
2. Нет, но для отправки срочных
3. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
4. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
5. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

Перечень контрольных заданий и (или) вопросов для оценки сформированности компетенций ОПК-5 (контролируемый индикатор достижения компетенции ОПК-5.3)

1. ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТ В СООТВЕТСТВИИ С ЗАКОНАДЕЛЬСТВОМ РФ:
1. Информация составляющая государственную тайну
2. Информация составляющая коммерческую тайну

3. Персональная
4. Конфиденциальная информация
5. Документированная информация

2. ДЛЯ ТОГО ЧТОБЫ СНИЗИТЬ ВЕРОЯТНОСТЬ УТРАТЫ ИНФОРМАЦИИ НЕОБХОДИМО:

1. Регулярно производить антивирусную проверку компьютера
2. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
3. Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)
4. Защитить вход на компьютер к данным паролем
5. Проводить периодическое обслуживание ПК

3. ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ ДОЛЖЕН

1. Содержать цифры и буквы, знаки препинания и быть сложным для угадывания
2. Содержать только цифры
3. Содержать только буквы
4. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
5. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

4. УСТРОЙСТВО ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ПРЕДСТАВЛЯЮЩЕЕ СОБОЙ МОБИЛЬНОЕ ПЕРСОНАЛЬНОЕ УСТРОЙСТВО, НАПОМИНАЮЩИЕ МАЛЕНЬКИЙ ПЕЙДЖЕР, НЕ ПОДСОЕДИНЯЕМЫЕ К КОМПЬЮТЕРУ И ИМЕЮЩИЕ СОБСТВЕННЫЙ ИСТОЧНИК ПИТАНИЯ:

1. Токен
2. Автономный токен
3. USB-токен
4. Устройство iButton
5. Смарт-карта

5. «ПЕРСОНАЛЬНЫЕ ДАННЫЕ» ЭТО:

1. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
2. Фамилия, имя, отчество физического лица
3. Год, месяц, дата и место рождения, адрес физического лица
4. Адрес проживания физического лица
5. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»