

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Кандрашина Елена Александровна

Должность: Врио ректора ФГАОУ ВО «Самарский государственный экономический университет»

Дата подписания: 02.08.2023 13:30:46

Уникальный программный ключ:

b2fd765521f4c570b8c6e8e502a10b4f1de8ae0d

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Самарский государственный экономический
университет»

Факультет среднего профессионального и предпрофессионального образования
Кафедра факультета среднего профессионального и предпрофессионального образования

АННОТАЦИЯ

Наименование дисциплины ОП.16 Кибербезопасность

Специальность 09.02.07 Информационные системы и программирование

Квалификация (степень) выпускника специалист по информационным системам

Самара 2023

1. Общая характеристика рабочей программы дисциплины «Кибербезопасность»

1.1. Место дисциплины в структуре основной образовательной программы:

Дисциплина ОП.17 «Кибербезопасность» является обязательной частью общепрофессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.07 «Информационные системы и программирование».

Дисциплина ОП.17 «Кибербезопасность» обеспечивает формирование общих компетенций в соответствии с ФГОС по специальности СПО 09.02.07 «Информационные системы и программирование».

Особое значение дисциплина имеет при формировании и развитии

ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6.
ПК 5.7

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.

Перечень профессиональных компетенций:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 5	<i>Проектирование и разработка информационных систем</i>
ПК 5.1	Собирать исходные данные для разработки проектной документации на информационную систему.
ПК 5.2	Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.
ПК 5.3	Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.
ПК 5.4	Производить разработку модулей информационной системы в соответствии с техническим заданием.
ПК 5.5	Осуществлять тестирование информационной системы на этапе опытной эксплуатации с фиксацией выявленных ошибок кодирования в разрабатываемых модулях информационной системы.
ПК 5.6	Разрабатывать техническую документацию на эксплуатацию информационной системы.
ПК 5.7	Производить оценку информационной системы для выявления возможности ее модернизации.

1.2. Планируемые результаты освоения дисциплины:

В результате изучения дисциплины обучающийся должен:

<i>уметь</i>	<ul style="list-style-type: none">– применять законы и другие нормативно-правовые акты в сфере информационной безопасности;– выявлять угрозы конфиденциальности, целостности, доступности информации;– принимать решения по обеспечению информационной безопасности.
<i>знать:</i>	<ul style="list-style-type: none">– средства и методы предотвращения и обнаружения вторжений;– технические каналы утечки информации;– возможности технических средств перехвата информации;– способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;– действующее законодательство РФ в информационной сфере;– государственную политику в сфере обеспечения информационной безопасности.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы учебной дисциплины	72
в том числе:	
теоретическое обучение	32
практические занятия	26
лабораторные занятия	-
курсовая работа (проект) <i>(не предусмотрено)</i>	
<i>Самостоятельная работа</i>	14
Промежуточная аттестация	Дифференцированный зачет

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся	Объем в часах
1	2	3
Раздел 1. Основные положения теории информационной безопасности		10
Тема 1.1. Основные понятия и задачи информационной безопасности	Содержание учебного материала	6
	Теоретическое обучение. Стандарты в области кибербезопасности. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность. Понятие нарушителя кибербезопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.	4
	В том числе практических занятий	2
	Практическое занятие. Работа в справочно-правовой системе с нормативными и правовыми документами по кибербезопасности	2
Тема 1.2. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	Содержание учебного материала	4
	Теоретическое обучение. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны. Схема построения кибербезопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения кибербезопасности государства. Военные подразделения в сфере кибербезопасности.	4
Раздел 2. Угрозы кибербезопасности		18
Тема 2.1. Классификация нарушений кибербезопасности вычислительной	Содержание учебного материала	8
	Теоретическое обучение. Понятие нарушения безопасности. Причины нарушения кибербезопасности. Аудит событий в рамках информационной системы. Уязвимости. Методы оценки уязвимости информации.	4
	В том числе практических занятий	4

системы и причины, обуславливающие их существование	Практическое занятие. Определение угроз объекта информатизации и их классификация.	4
Тема 2.2. Анализ способов нарушений кибербезопасности	Содержание учебного материала	10
	Теоретическое обучение. Анализ различных способов нарушений кибербезопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем. Каналы и методы несанкционированного доступа к информации.	4
	В том числе практических занятий	6
	Практическое занятие. Выполнение индивидуального задания по теме: «Способы нарушений кибербезопасности»	6
Раздел 3. Организационные и технические меры по обеспечению защиты информации		30
Тема 3.1. Защита информации в автоматизированных (информационных) системах	Содержание учебного материала	8
	Теоретическое обучение. Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.	4
	В том числе практических занятий	4
	Практическое занятие. Выбор мер защиты информации для автоматизированного рабочего места.	4
Тема 3.2. Методы криптографии	Содержание учебного материала	10
	Теоретическое обучение. Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии. Электронная подпись.	4
	В том числе практических занятий	6
	Практическое занятие. Выбор мер защиты информации для автоматизированного рабочего места.	6

Тема 3.3. Основные технологии построения защищенных систем	Содержание учебного материала	8
	Теоретическое обучение. Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.	4
	В том числе практических занятий	4
	практическое занятие. Проектирование системы безопасности автоматизированной информационной системы с описанием возможных угроз и оценкой вероятности их возникновения	4
Тема 3.4. Место кибербезопасности экономических систем в национальной безопасности страны	Содержание учебного материала	4
	Теоретическое обучение. Информационная безопасность страны. Защита экономических систем. Обмен конфиденциальной информацией. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов. Концепция кибербезопасности. Основные сведения и положения.	4
Тематика самостоятельной учебной работы 1. Работа с конспектами, учебной и специальной литературой; 2. Доработка разрабатываемых проектов; 3. Подготовка отчетов по практическим занятиям; 4. Написание рефератов и докладов.		14
Курсовой проект (работа) (не предусмотрена)		
Самостоятельная учебная работа обучающегося над курсовым проектом (работой) (не предусмотрена)		
Консультация		-
Промежуточная аттестация (Дифференцированный зачет)		Дифференцированный зачет
Всего		72

