МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ:

Директор центра
делового образования
ФГБОУ ВО «СГЭУ»,
д.п.н., профессор
_____ Э.П. Печерская
«__» _____2020г.

РАБОЧАЯ ПРОГРАММА ПО ДИСЦИПЛИНЕ

«Информационная безопасность»

Наименование программы профессиональной переподготовки «Преподаватель профессионального образования»

Программу разработал: Ромодина В.В., преподаватель ФГБОУ ВО «СГЭУ».

САМАРА – 2020

1. Цели и задачи дисциплины «Информационная безопасность»

1.1 Цель изучения дисциплины «Информационная безопасность»: ознакомить слушателей с принципами решения задач обеспечения информационной безопасности компьютерных систем. изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

1.2 Основными задачами изучения дисциплины являются:

-понимать место информационной безопасности в системе национальной безопасности РФ;

-изучить угрозы информационной безопасности;

-освоить современные подходы к построению систем защиты информации;

-изучить особенности обеспечения информационной безопасности компьютерных систем;

- изучить разновидностях информации ограниченного доступа.

1.3 Требования к результатам освоения дисциплины:

В результате освоения программы слушатель должен обладать следующими профессиональными компетенциями:

- способностью обеспечивать безопасность и целостность данных информационных систем и технологий (ПК-31).

По окончании освоения дисциплины обучающийся должен:

Знать:

- 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; организацию защиты информации от утечки по техническим каналам на объектах информатизации;

Уметь:

- пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения;

Владеть:

- методами и средствами технической защиты информации;

-методами расчета и инструментального контроля показателей технической защиты информации.

2. Содержание дисциплины

п/п	Наименование учебных тем	Трудоемкость, (час.)	В том числе		Самостоятельная работа (час.)	Форма контроля
			Лекции, (час.)	Практические занятия, (час.)		
1.	Информационная безопасность в условиях функционирования в России глобальных сетей.	10			10	
2.	Модели безопасности и их применение.	10			10	
3.	Защита информации	10			10	
4.	Информационная безопасность	8			8	

	экономических систем в национальной безопасности страны					
	Итоговое тестирование	2				зачет
	ИТОГО:	40				

СОДЕРЖАНИЕ ТЕМ

Тема 1. Информационная безопасность в условиях функционирования в России глобальных сетей. Стандарты в области информационной безопасности. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация. Три вида возможных нарушений информационной безопасности. 3 составляющих ИБ - целостность, доступность, конфиденциальность. Защита информационной системы от угроз. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны.
Тема 2. Модели безопасности и их применение. Понятие таксономии нарушения безопасности. Причины нарушения информационной безопасности. Аудит событий в рамках информационной системы. Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.
Тема 3. Защита информации. Защищенные компьютерные системы. Их виды и особенности. Примеры защищенных систем. Их использование и применение на практике. Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии. Электронная цифровая подпись. 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.
Тема 4. Информационная безопасность экономических систем в национальной безопасности страны. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. 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 информационной безопасности. Основные сведения и положения.

3. Форма аттестации

Форма итоговой аттестации - *зачет* (тестирование)

4.Оценочные материалы дисциплины

Цель – оценить уровень усвоения знаний по программе.

Процедура: тестирование проводится с использованием «Системы управления обучением СГЭУ». Слушателям предлагается для ответа 17 вопросов по разделам программы, предполагающие выбор варианта ответа.

№ п/п	Формулировка вопроса и варианты ответа
1.	Эффективная программа безопасности требует сбалансированного применения: а) контрмер и защитных механизмов б) процедур безопасности и шифрования в) технических и нетехнических методов
2.	Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют: а) уровень доверия, обеспечиваемый механизмом безопасности б) внедрение управления механизмами безопасности в) классификацию данных после внедрения механизмов безопасности
3.	Что такое политика безопасности: а) детализированные документы по обработке инцидентов безопасности б) широкие, высокоуровневые заявления руководства в) общие руководящие требования по достижению определенного уровня безопасности
4.	Для чего создаются информационные системы: а) получения определенных информационных услуг б) обработки информации в) оба варианта верны
5.	Конфиденциальностью называется: а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов б) описание процедур в) защита от несанкционированного доступа к информации
6.	Информационная безопасность зависит от: а) компьютеров, поддерживающей инфраструктуры б) пользователей в) информации
7.	Защита информации: а) небольшая программа для выполнения определенной задачи б) комплекс мероприятий, направленных на обеспечение информационной безопасности в) процесс разработки структуры базы данных в соответствии с требованиями пользователей
8.	Под информационной безопасностью понимается: а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре б) программный продукт и базы данных должны быть защищены по нескольким направ-лениям от воздействия в) нет верного ответа
9.	Какой вид идентификации и аутентификации получил наибольшее распространение: а) системы PKI б) постоянные пароли в) одноразовые пароли

10.	Таргетированная атака – это: а) атака на сетевое оборудование б) атака на компьютерную систему крупного предприятия в) атака на конкретный компьютер пользователя
11.	Stuxnet – это: а) троянская программа б) макровирус в) промышленный вирус
12.	Какие вирусы активизируются в самом начале работы с операционной системой: а) загрузочные вирусы б) троянцы в) черви
13.	Системой криптографической защиты информации является: а) BFox Pro б) CAudit Pro в) Крипто Про
14.	Какой подход к обеспечению безопасности имеет место: а) теоретический б) комплексный в) логический
15.	Какие угрозы безопасности информации являются преднамеренными: а) ошибки персонала б) открытие электронного письма, содержащего вирус в) не авторизованный доступ
16.	. Под какие системы распространение вирусов происходит наиболее динамично: а) Windows б) Mac OS в) Android
17.	Заключительным этапом построения системы защиты является: а) сопровождение б) планирование в) анализ уязвимых мест

Шкала и критерии тестирования

Минимальный ответ (% правильных ответов) и оценка 2	Изложенный, раскрытый ответ (% правильных ответов) и оценка 3	Законченный, полный ответ (% правильных ответов) и оценка 4	Образцовый; достойный подражания ответ (% правильных ответов) и оценка 5
50% и менее	51-71%	72-92%	93-100%

5. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. - 3-е изд. (эл.). - М. : БИНОМ, 2015. - (Программисту). - http://www.studentlibrary.ru/book/ISBN9785996329526.html Электронное издание на основе: Криптография и безопасность в технологии .NET [Электронный ресурс] / П. Торстейнсон, Г. А. Ганеш ; пер. с англ.-3-е изд. (эл.).- Электрон. текстовые дан. (1 файл pdf : 482 с.).- М. : БИНОМ. Лаборатория знаний, 2015.- (Программисту).-Систем. требования: Adobe Reader XI ; экран 10". - ISBN 978-5-9963-2952-6.
2. Интеллектуальные системы защиты информации [Электронный ресурс]: учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html Электронное издание на основе: Интеллектуальные системы защиты информации: учеб. пособие/ В. И. Васильев. 2-е изд., испр. и доп. - М.: Машиностроение, 2013.- 172 с. - ISBN 978-5-94275-667-3. 11
3. Информатика 2015 [Электронный ресурс] : учебное пособие / Алексеев А.П. - М. : СОЛОН-ПРЕСС, 2015. - ttp://www.studentlibrary.ru/book/ISBN9785913591586.html Электронное издание на основе: Информатика 2015: учебное пособие/ Алексеев А.П.- 2015. - 400 с., илл. - ISBN 978-5-91359-158-6.
4. Балдин К. В. Информационные системы в экономике. — Москва: Дашков и К 2015 г.— 395 с. —УМО- Электронное издание. — ISBN 978-5-394-01449-9 http://ibooks.ru/product.php?productid=342405

Дополнительная литература:

1. Зараменских, Е. П. Управление жизненным циклом информационных систем : учебник и практикум для академического бакалавриата / Е. П. Зараменских. — Москва : Издательство Юрайт, 2019. — 431 с. — (Бакалавр. Академический курс). — ISBN 978-5-9916-9200-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433676
2. Иванов В. Microsoft Office System 2003: Учебный курс. – Питер; Киев:Издательская группа BHV, 2004.
3. Информационные технологии в экономике и управлении в 2 ч. Часть 1 : учебник для академического бакалавриата / В. В. Трофимов [и др.] ; под редакцией В. В. Трофимова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 269 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-09083-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/442379
4. Информационные технологии в экономике и управлении в 2 ч. Часть 2 : учебник для академического бакалавриата / В. В. Трофимов [и др.]. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 245 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-09084-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/442380
5. Лапчик М.П., Семакин И.Г., Хеннер Е.К. Методика преподавания информатики: Учебн. пособие для студ.педвузов.-М.:Изд. центр «Академия».
6. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2006. – 958 с.: ил.
7. Основы современных компьютерных технологий: Учебное пособие / Под ред. проф. Хомоненко А.Д.. – СПб.: КОРОНА, 2002.
8. Педагогические технологии дистанционного обучения: Учеб. пособие для студ. высш. пед. учеб. заведений / Е.С.Полат [и др.]; Под ред. Е.С.Полат. – М.: Издательский центр «Академия», 2006. – 400 с.

9. Стружкин, Н. П. Базы данных: проектирование : учебник для академического бакалавриата / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2019. — 477 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-00229-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432177
10. Стружкин, Н. П. Базы данных: проектирование. Практикум : учебное пособие для академического бакалавриата / Н. П. Стружкин, В. В. Годин. — Москва : Издательство Юрайт, 2019. — 291 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-00739-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433865

Ресурсы информационно-телекоммуникационной сети «Интернет»:

Государственные и региональные органы:

1. http://government.ru/ официальный сайт Правительства РФ.
2. http:// www.consultant.ru «Консультант плюс»
3. http://www.garant.ru «Гарант»
4. http://www.elibrery.ru «Научная электронная библиотека»
5. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)
6. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - http://www.gks.ru/)