Министерство просвещения Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ФТД.03 «ЦИФРОВАЯ БЕЗОПАСНОСТЬ»

Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)

Профиль программы «Информационные технологии (по элективным модулям*)»

Автор(ы): ст. преп. С.В. Ченушкина

Одобрена на заседании кафедры информационных систем и технологий. Протокол от «20» января 2022 г. №5.

Рекомендована к использованию в образовательной деятельности научно-методической комиссией института ИПО РГППУ. Протокол от «26» января 2022 г. №6.

Екатеринбург
2022

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины «Цифровая безопасность»: изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах

Задачи:

- определение целей и принципов цифровой защиты информации
- изучение современной доктрины информационной безопасности
- рассмотрение состава защищаемой информации, ее классификацией по видам тайн, материальным носителям, собственникам и владельцам
- установление структуры угроз защищаемой информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Цифровая безопасность» относится к факультативным дисциплинам учебного плана.

Для изучения учебной дисциплины необходимы знания, умения и владения, формируемые следующими дисциплинами:

1. Архитектура ПК и периферийные устройства.
2. Ознакомительная практика.
3. Операционные системы.
4. Компьютерные коммуникации и сети.

Перечень учебных дисциплин, для которых необходимы знания, умения и владения, формируемые данной учебной дисциплиной:

1. Информационные технологии прогнозирования и оптимизации в бизнесе.
2. Организационно-правовое обеспечение информационной безопасности.
3. Основы создания и эксплуатации защищенных компьютерных систем.
4. Российские и международные стандарты информационной безопасности.
5. Соадминистрирование баз данных и серверов.

3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина направлена на формирование следующих компетенций:

- ПКО-6 Способен модернизировать и использовать возможности образовательной среды для достижения личностных, учебно-профессиональных результатов обучения и обеспечения качества образовательного процесса;
- ПКС-2.1 Способен проводить работы по установке и техническому обслуживанию средств защиты информации;

- ПКС-2.3 Способен вести техническую документацию, связанную с эксплуатацией систем защиты информации автоматизированных систем;
- ПКС-5.3 Способен обслуживать средства защиты информации в компьютерных системах и сетях.

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

З1. Теорию информационной безопасности, методологию защиты информации;

З2. Правовое обеспечение информационной безопасности, законодательную базу, систему государственного контроля и управления в области информационной безопасности;

З3. Организационное обеспечение информационной безопасности;

З4. Основные программные средства защиты информации;

З5. Криптографические методы и средства обеспечения информационной безопасности.

Уметь:

У1. Оценивать состояние организационной защиты информации на объекте;

У2. Определять рациональные меры по обеспечению организационной защите на объекте;

У3. Организовать работу с персоналом с секретной (конфиденциальной) информацией.

Владеть:

В1. Методами выявления угроз информационной безопасности объекта;

В2. Способами обеспечения режима и секретности на объекте.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоёмкость дисциплины составляет 2 зач. ед. (72 час.), семестр изучения – 6, распределение по видам работ представлено в табл. № 1.

Таблица 1. Распределение трудоемкости дисциплины по видам работ

Вид работы	Форма обучения
	очная
	Семестр изучения
	6 сем.
	Кол-во часов
Общая трудоемкость дисциплины по учебному плану	72

Контактная работа, в том числе:	22
Практические занятия	22
Самостоятельная работа студента	50
Промежуточная аттестация, в том числе:	
Зачет	6 сем.

**Распределение трудоемкости по видам контактной работы для заочной формы обучения (при наличии) корректируется в соответствии с учебным планом заочной формы обучения.*

4.2 Содержание и тематическое планирование дисциплины

Таблица 2. Тематический план дисциплины

Наименование разделов и тем дисциплины (модуля)	Сем.	Всего, час.	Вид контактной работы, час.			СРС
			Лекции	Практ. занятия	Лаб. работы	
1. Основные цели и задачи курса.	6	8	-	2	-	6
2. Угрозы информационной безопасности на предприятии	6	12	-	4	-	8
3. Методы и средства защиты информации	6	26	-	10	-	16
4. Базовые нормативные документы по цифровой информации	6	12	-	2	-	10
5. Документационное обеспечение цифровой безопасности на предприятии	6	14	-	4	-	10

**Распределение часов по разделам (темам) дисциплины для заочной формы обучения осуществляется научно-педагогическим работником, ведущим дисциплину.*

4.3 Содержание разделов (тем) дисциплин

Раздел 1. Основные цели и задачи курса.

Актуальность цифровой безопасности. Основные цели и задачи системы защиты. Источники угроз и атак. Основные классификации атак. Системы критериев оценки защищенности среды.

Раздел 2. Угрозы информационной безопасности на предприятии

Виды угроз цифровой безопасности и их характеристика. Модели нарушителей цифровой безопасности на предприятии. Формы преступного

посягательства. Оценка ущерба вследствие организационных нарушений цифровой безопасности на предприятии.

Раздел 3. Методы и средства защиты информации

Требования к защите информации, изложенные в соответствующих Законах РФ, стандартах и нормативных документах. Сравнение с нормативными документами о защите информации и мер наказания нарушителей законов о защите информации в развитых странах.

Технические мероприятия, призванные обеспечить физическую и информационную безопасность. Технические средства для реализации мероприятий данной группы.

Программные средства защиты информации. Задачи обеспечения конфиденциальности, целостности и задачи обеспечения наблюдаемости, решаемые программными средствами защиты информации.

Обеспечение безопасности электронного документооборота. Электронная подпись. Методы и средства защиты информации при работе с удаленными базами данных. Стеганография. Компьютерные вирусы и программы типа «Троянский конь». Средства обнаружения и уничтожения компьютерных вирусов.

Раздел 4. Базовые нормативные документы по цифровой информации

Мировая нормативная практика по защите информации в информационных системах. Европейское законодательство о защите информации и персональных данных. Конституция РФ о защите информации и гарантии прав на информацию. Доктрина информационной безопасности РФ, принципы и методы защиты информации. ФЗ «Об информации, информационных технологиях и о защите информации», классификация информации, права и обязанности обладателя информации. ФЗ «О персональных данных», понятие и состав персональных данных, особенности их защиты и передачи по каналам связи. ФЗ Закон РФ «О государственной тайне». ФЗ «О техническом регулировании», понятие и требования аккредитации и сертификации. ФЗ «О лицензировании отдельных видов деятельности», понятие, виды лицензируемой деятельности, контроль за лицензируемой деятельностью.

Раздел 5. Документационное обеспечение цифровой безопасности на предприятии

Перечень и содержание основных документов, необходимых при построении системы защиты в организации: приказы, распоряжения, перечни, матрицы, модели, акты, технические паспорта, схемы контролируемых зон, методические пособия, памятки, журналы. Перечень документов заявителя для аттестации автоматизированной системы и типовые формы. Некоторые рекомендации по проведению мероприятий по защите информации и выбору параметров защиты.

Порядок деятельности по осуществлению требований организационно-распорядительной документации, периоды проверок, составы комиссий, привлечение аттестованных организаций. Рекомендации по составлению отчетности и ведению журналов учета доступа и СКЗИ.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для изучения дисциплины используются различные образовательные технологии:

1. Основными целями контрольной работы являются: практическое применение теоретических знаний, полученных в процессе изучения дисциплины; выявление степени изучения и усвоения студентом программного материала; привития ему первичных навыков самостоятельной работы, связанной с поиском, научной и учебной литературы; формирование способностей к анализу и объективной оценке исследуемого научного и практического материала.

Выполнение контрольной работы предполагает углубление и систематизацию полученных знаний по изучаемому курсу в целом и по избранной теме в частности; выработку навыков сбора и обобщения практического материала, работы с первоисточниками; развитие умений применять полученные знания для решения конкретных научных и практических проблем, формулировать и аргументировать собственную позицию в их решении.

Материалы необходимые для выполнения контрольной работы располагаются на кафедре и в электронной информационно-образовательной среде (ЭИОС).

2. Последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

3. Организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

4. При реализации образовательной программы с применением дистанционных образовательных технологий и электронного обучения:

- состав видов контактной работы по дисциплине (модулю), при необходимости, может быть откорректирован в направлении снижения доли занятий лекционного типа и соответствующего увеличения доли консультаций (групповых или индивидуальных) или иных видов контактной работы;
- информационной основой проведения учебных занятий, а также организации самостоятельной работы обучающихся по дисциплине (модулю) являются представленные в электронном виде методические, оценочные и иные материалы, размещенные в электронной информационно-образовательной среде (ЭИОС) университета, в электронных библиотечных системах и открытых Интернет-ресурсах;

- взаимодействие обучающихся и педагогических работников осуществляется с применением ЭИОС университета и других информационно-коммуникационных технологий (видеоконференцсвязь, облачные технологии и сервисы, др.);

- соотношение контактной и самостоятельной работы по дисциплине (модулю) может быть изменено в сторону увеличения последней, в том числе самостоятельного изучения теоретического материала.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1 Основная литература

1. Шаньгин В. Ф. Информационная безопасность и защита информации : учебное пособие. - Саратов : Профобразование, 2017. - 702 с. - Режим доступа: http://www.iprbookshop.ru/63594.

2. Костюк А. В. Информационные технологии. Базовый курс: учебник / Костюк А. В., Бобонец С. А., Флегонтов А. В. — Санкт-Петербург : Лань, 2018. — 604 с. — Режим доступа: http://e.lanbook.com/book/104884.

3. Никифоров С. Н. Методы защиты информации. Защищенные сети: учебное пособие / Никифоров С. Н. — Санкт-Петербург : Лань, 2018. — 96 с. — Режим доступа: http://e.lanbook.com/book/110935.

4. Степанова, Е. Н. Организация и сопровождение электронного документооборота : практикум для СПО / Е. Н. Степанова. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2021. — 176 с. — ISBN 978-5-4488-1275-0, 978-5-4497-1042-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/107183.html

5. Никифоров С. Н. Методы защиты информации. Шифрование данных: учебное пособие / Никифоров С. Н. — Санкт-Петербург : Лань, 2018. — 160 с. — Режим доступа: http://e.lanbook.com/book/106734.

6. Шаврин С. С. Реализация базовых операций защиты информации на сигнальных процессорах. Часть 2 : учебное пособие. - Москва : Московский технический университет связи и информатики, 2016. - 41 с. - Режим доступа: http://www.iprbookshop.ru/61539.

6.2 Дополнительная литература

1. Петров А. А. Компьютерная безопасность. Криптографические методы защиты : монография. - Саратов : Профобразование, 2017. - 446 с. - Режим доступа: http://www.iprbookshop.ru/63800.

6.3 Программное обеспечение и Интернет-ресурсы

Интернет-ресурсы:

1. Интернет-портал по информационной безопасности. Режим доступа: https://infobezlikbez.ru/

2. Совет Безопасности РФ. Режим доступа: http://www.scrf.gov.ru

3. ITSec.Ru - портал для профессионалов информационной безопасности. Режим доступа: http://www.itsec.ru/

Программное обеспечение:

1. Операционная система Windows.
2. Офисная система Office Professional Plus.
3. Операционная система Ubuntu.
4. Программное обеспечение виртуализации VM VirtualBox.

Информационные системы и платформы:

1. Система дистанционного обучения «Moodle».
2. Информационная система «Таймлайн».
3. Платформа для организации и проведения вебинаров «Mirapolis Virtual Room».

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень материально-технического обеспечения для реализации образовательного процесса по дисциплине:

1. Учебная аудитория для проведения занятий лекционного типа.
2. Компьютерный класс.
3. Учебная аудитория для проведения занятий семинарского (практического) типа, проведения групповых и индивидуальных консультаций, проведения текущего контроля и промежуточной аттестации.
4. Помещения для самостоятельной работы.