АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
Б1.О.10.05 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Автор: к.т.н.. доцент кафедры системного анализа и информатики
Каширская Е.Н.
Направление подготовки:09.03.03 «Прикладная информатика»
Направленность: «Прикладная информатика в энергетических системах»
Квалификация выпускника: бакалавр
Формы обучения: очно-заочная

Цели и задачи дисциплины (модуля).

Дисциплина «Информационная безопасность» предназначена для повышения уровня образованности в области прикладной информатики, которая изучает связь таких предметов, как «Вычислительные системы. сети и телекоммуникации», «Сетевое администрирование», «Объектно-ориентированное программирование» и др. и предназначена для отработки навыков настройки операционных систем с целью повышения надежности работы компьютера, а также не допустить потери информации и ее утечки.

В соответствии с назначением основной целью дисциплины является ознакомление студентов гуманитарных направлений с общими представлениями о фундаментальных понятиях, используемых в данном курсе, основами защиты сетей, операционных систем и их управлением, обучение работе с пакетом прикладных программ, научно-технической литературой и технической документацией.

Исходя из цели, в процессе изучения дисциплины решаются следующие задачи:

- - научить студентов разбираться в терминологии и понятиях, получение обучающимися общего представления о задачах информационной безопасности с акцентом на управление современными ИТ инфраструктурами без привязки к одной какой-либо сетевой операционной системе.
- - объяснить студентам все основные аспекты защищенной работы в Интернете, с электронной почтой, надежную защиту файлов и документов от несанкционированного доступа, эффективной борьбы с вирусами, троянскими программами, современное предотвращение, а также быстрое противодействие атакам взломщиков, оптимальной политики безопасности пользователей и решение их проблем.
- - изменить, по возможности, мировоззрение будущих специалистов – экономистов, политиков и бизнесменов в принципиальном отношении к использованию защищенной работы в сетях.

План курса

№ п/п	Название темы	Основные вопросы и положения, раскрывающие содержание темы
Тема 1	Актуальность информационной безопасности в современных условиях	Что такое информационная безопасность. Актуальность проблемы информационной безопасности. Понятия и определения в информационной безопасности.
Тема 2	Угрозы и возможные каналы утечки конфиденциальной информации.	Основные закономерности возникновения и классификация угроз информационной безопасности.

		Пути и каналы утечки информации и их обобщенная модель. Классификация каналов утечки информации.
Тема 3	Компьютерные вирусы и деструктивные программы.	Классификация компьютерных вирусов. Файловые вирусы. Загрузочные вирусы. Макровирусы. Сетевые вирусы. Прочие вредные программы.
Тема 4	Методы защиты информации в автоматизированных системах обработки данных.	Откуда берутся компьютерные вирусы. Основные правила защиты от компьютерных вирусов. Антивирусные программы. Восстановление пораженных компьютерными вирусами объектов.
Тема 5	Стандарты безопасности компьютерных систем.	Критерии безопасности компьютерных систем. "Оранжевая книга". Руководящие документы Гостехкомиссии. Краткий обзор современных методов защиты информации. Ограничение доступа. Контроль доступа к аппаратуре. Разграничение и контроль доступа к информации АСОД. Разграничение привилегий на доступ. Идентификация и установление подлинности объекта. Криптографическое преобразование информации. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
Тема 6	Обеспечение информационной безопасности в Интернет.	Примеры взломов сетей и Web-узлов. Пользователи и злоумышленники в Internet. Причины уязвимости сети Internet. Обеспечение информационной безопасности организации при ее подключении к Internet. Защита архитектуры клиент/сервер
Тема 7	Сеть интранет как основной объект нападений из Интернет.	Удаленные атаки на интрасети. Классические методы взлома интрасетей. Современные методы взлома интрасетей. Улучшение паролей. Одноразовые пароли. Серверы аутентификации. Физическая изоляция. Изоляция протокола. Выделенные каналы и маршрутизаторы. Защита систем управления базами данных. Защита в сетевых операционных системах.

Формы текущего контроля промежуточной аттестации

По окончанию изучения дисциплины «Информационная безопасность» студент должен:

- знать:

- состояние исследований в России и в мире по затронутой проблеме;
- основные понятия и информативные документы России по информационной безопасности
- модели угроз со стороны нарушителя безопасности информационной системы;
- организации и нормативные документы, действующие в России;
- схему оформления документов на право получения соответствующих лицензий на производство и использование программных продуктов

- уметь:

- строить модель угроз нарушителя применительно к конкретной информационной системе;
- правильно пользоваться программными и аппаратными ресурсами предприятия с целью обеспечения информационной безопасности информационной системы;
- правильно действовать в условиях использования вычислительной техники и программного обеспечения, что особенно характерно для настоящего времени;
- реализовывать правильно схему обеспечения на предприятии информационной безопасности.

- владеть навыками

- защищенной работы в Интернет
- работы с электронной почтой,
- надежной защитой файлов и документов от несанкционированного доступа,
- эффективной борьбы с вирусами, троянскими программами,
- своевременного предотвращения, а также быстрого противодействия атакам взломщиков,
- оптимальной политики безопасности пользователей и решение их проблем.

Планируемые результаты обучения по дисциплине (модулю) «Информационная безопасность»

Код компетенции	Содержание компетенции	Планируемые результаты обучения по дисциплине (модулю)
УК ОС-2	Способность разработать проект на основе оценки ресурсов и ограничений	на уровне знаний: знать способы оценки ресурсов и ограничений.
		на уровне умений: уметь опираться на имеющиеся ресурсы и ограничения при разработке проектов
		на уровне навыков: разрабатывать проекты информационных систем с учетом имеющихся ресурсов и наложенных ограничений
ОПК-3	способность решать стандартные задачи профессиональной	на уровне знаний: знать задачи в области профессиональной

	деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	деятельности и требования информационной безопасности;
		на уровне умений: решать стандартные задачи на основе информационной культуры и применять информационные технологии;
		на уровне навыков: владеть способами решения стандартных задач и информационными технологиями.
ОПК-4	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	на уровне знаний: знать методы решения стандартных задач профессиональной деятельности
		на уровне умений: уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры
		на уровне навыков: выполнять основные требования информационной безопасности при проектировании информационных систем.

Объем дисциплины (модуля) «Информационная безопасность» для очно-заочной формы

Вид учебной работы		Количество часов										
		Всего по уч. плану	Семестр									
			1	2	3	4	5	6	7	8	9	10
аудиторные занятия (всего):		**48**						48				
в том числе	лекционные занятия	**16**						16				
	практические занятия	**32**						32				
самостоятельная работа:		**132**						132				
общая трудоемкость дисциплины:	**часы:**	**216**						180				
	зачетные единицы:	**6**						5				
Формы итогового контроля		**экзамен**						36 ч.				

Основная литература

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов :

Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 c. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72341.htm

2. Бондарев В. Введение в информационную безопасность автоматизированных систем. М.: МГТУ им. Н. Э. Баумана, 2016. 252 с.
3. Бабаш А., Баранова Е. Информационная безопасность и защита информации. М.: Инфра-М, 2016. 324 с.
4. Шаньгин В.С. Информационная безопасность компьютерных сетей и систем: учеб. пособие. М.: ИД «Форум» - Инфра-М, 2011. 416 с. Электронный ресурс: http://www.ipa.nw.ru/PAGE/aspirantura/literatura/shangin.pdf.

Дополнительная литература

1. Бабаш А., Баранова Е., Ларин Д. Информационная безопасность. История защиты информации в России. М.: КДУ, 2015. 736 с.
2. Бирюков А. Информационная безопасность: защита и нападение. 2-е изд. М.: ДМК Пресс, 2017. 474 с. Электронный ресурс: https://vk.com/doc219780081_439946298.
3. Фергюсон Н., Шнайер Б. Практическая криптография. М.: Вильямс, 2017. 420 с.
4. Нестеров С.А. Основы информационной безопасности. М.: Лань, 2016. 324 с.