БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе
и образовательным инновациям
_____ О.Г. Прохоренко
«30» июня 2022 г.

Регистрационный № УД- 11175 /уч.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-25 01 12 Экономическая информатика

2022 г.

Учебная программа составлена на основе ОСВО 1-25 01 12-2013, учебного плана рег. № Е25-289/уч. от 16.03.2020.

СОСТАВИТЕЛЬ:
В. А. Макаревич, преподаватель кафедры цифровой экономики экономического факультета Белорусского государственного университета, магистр управления.

РЕЦЕНЗЕНТ:
А.Д. Луцевич, канд. экон. наук, доцент, заведующий кафедрой управления экономическими системами Академии управления при Президенте Республики Беларусь

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой цифровой экономики
(протокол № 10 от 29.06.2022);
Научно-методическим Советом БГУ
(протокол № 6 от 29.06.2022)

Зав.кафедрой цифровой экономики _____И.А. Карачун

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Цель учебной дисциплины – формирование системы теоретических знаний в области информационной безопасности и овладение практическими навыками использования методов и средств защиты информации.

Задачи учебной дисциплины:

1. Раскрыть основные понятия и категории в области информационной безопасности.
2. Ознакомить с основными инструментами и стратегиями защиты информации и объектов информатизации.
3. Ознакомить с моделями и принципами безопасного поведения в сети Интернет и социальных сетях.
4. Изучить и овладеть практическими навыками по обеспечению защиты активов системы информационной безопасности организации.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием (магистра).

Учебная дисциплина «Информационная безопасность» относится к циклу общенаучных и общепрофессиональных дисциплин компонента учреждения высшего образования.

Требования к компетенциям

Освоение учебной дисциплины «Информационная безопасность» должно обеспечить формирование следующих академических, социально-личностных и профессиональных компетенций:

академические компетенции:

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным порождать новые идеи (обладать креативностью).

АК-6. Владеть междисциплинарным подходом при решении проблем.

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

социально-личностные компетенции:

СЛК-2. Быть способным к социальному взаимодействию.

СЛК-3. Обладать способностью к межличностным коммуникациям.

СЛК-4. Владеть навыками здоровьесбережения.

СЛК-5. Быть способным к критике и самокритике.

СЛК-6. Уметь работать в команде.

профессиональные компетенции:

ПК-13. Оценивать эффективность решений в сфере информатизации.

ПК-14. Использовать информационные технологии для повышения эффективности обработки исходных данных, проведения математических и статистических расчётов, ведения документооборота и маркетинговых исследований.

ПК-26. Осуществлять проектирование, тестирование, сопровождение и эксплуатацию информационных систем, разрабатывать техническую документацию к программному обеспечению и требования к внедрению тиражируемых информационных систем.

ПК-27. Проводить научные исследования в области использования информационных технологий в экономике.

ПК-28. Проводить научные исследования с целью совершенствования методов проектирования, тестирования, оценки качества, внедрения и сопровождения прикладного программного обеспечения.

В результате освоения учебной дисциплины студент должен:

знать: современные законы, стандарты, методы, технологии и направления в области защиты информации; законодательство Республики Беларусь в области защиты информации; требования к защите информации определенного типа; иметь представление о значении информационной безопасности для организации в условиях цифровой трансформации экономики;

уметь: анализировать и применять модели информационной безопасности; использовать современные программно-аппаратные средства защиты информации; подбирать и обеспечивать защиту информации; разрабатывать проекты организационно-распорядительных документов, регламентирующих работу по защите информации;

владеть: методами организации и управления деятельностью служб защиты информации на предприятии; современными методами обеспечения защиты информации; современными средствами защиты информации; навыками безопасного поведения в сети Интернет.

Структура учебной дисциплины

Дисциплина изучается в 5 семестре дневной формы обучения. Всего на изучение учебной дисциплины «Информационная безопасность» отведено:

– для очной формы получения высшего образования – 140 часов, в том числе 66 аудиторных часа, из них: лекции – 28 часов, лабораторные занятия – 32 часа, УСР – 6 часов.

Трудоемкость учебной дисциплины составляет 4 зачетных единицы.

Форма текущей аттестации – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1 Введение в информационную безопасность

Информационная безопасность: понятие, подходы к определению, основные компоненты. Модели информационной безопасности, гексада Паркера, триада «Конфиденциальность-Целостность-Доступность». Атаки информационной безопасности: типы атак, угрозы, уязвимости и риски. Управление рисками и меры реагирования на чрезвычайные происшествия.

Тема 2 Идентификация и аутентификация

Идентификация: понятие, проверка личности, способы обхода идентификации. Аутентификация: понятие, основные факторы аутентификации. Виды аутентификации: многофакторная, взаимная. Методы идентификации и аутентификации: пароли, биометрические данные, аппаратные токены. Безопасность паролей.

Тема 3 Контроль доступа. Внедрение и основные модели

Контроль доступа: понятие и способы внедрения. Модели контроля доступа: дискреционный контроль доступа, обязательный контроль доступа, контроль доступа на основе правил, ролей и атрибутов, многоуровневый контроль доступа. Контроль физического доступа.

Тема 4 Отчетность и аудит

Отчетность: понятие, основные преимущества ведения отчетности. Аудит: понятие аудита, объекты аудита, основные методы аудита, ведение журналов, мониторинг, аудит с выполнением оценки.

Тема 5 Криптография

Криптография: понятие, история, элементарные шифры, скитала, атбаш, шифр Цезаря, криптографические машины, принципы Керкхоффса. Современные криптографические инструменты: шифры с ключевыми словами, одноразовые блокноты, симметричная и асимметричная криптография, хеш-функции, цифровые подписи и сертификаты. Защита данных в состоянии покоя, в движении и в процессе использования.

Тема 6 Соответствие требованиям, законодательство и нормативные положения

Соответствие: понятие, последствия несоответствия, меры достижения соответствия. Соблюдение нормативных требований. Законодательство Республики Беларусь в сфере информационной безопасности. Соответствие государственным и отраслевым нормативным требованиям. Выбор структуры для соответствия. Пользовательские структуры. Соответствие требованиям в условиях технологических изменений.

Тема 7 Операционная безопасность

Операционная безопасность: определение, истоки, законы, процесс обеспечения. Моделирование угроз: идентификация активов, анализ угроз, анализ уязвимостей, оценка рисков, генерация мер противодействия. Операционная безопасность в частной жизни.

Тема 8 Человеческий фактор в информационной безопасности

Социальная инженерия: понятие, разновидность, процесс атаки. Сбор информации для осуществления атак социальной инженерии. Типы атак социальной инженерии: претекстинг, фишинг, вишинг и пр. Обучение безопасности в организации: пароли, обучение социальной инженерии, использование сетей, вредоносное ПО, личное оборудование, политики и нормативные знания.

Тема 9 Физическая безопасность

Выявление физических угроз. Меры контроля физической безопасности. Сдерживающие меры: меры обнаружения, превентивные меры, меры контроля физического доступа. Защита людей: физические уязвимости персонала, обеспечение безопасности, эвакуация. Административные меры контроля. Защита данных и оборудования.

Тема 10 Сетевая безопасность

Защита сетей. Проектирование безопасных сетей и использование брандмауэров. Системы обнаружения сетевых вторжений. Защита сетевого трафика: виртуальные частные сети, беспроводные сети, использование безопасных протоколов. Инструменты сетевой безопасности: защита беспроводной сети, сканеры, снифферы пакетов, приманки, инструменты брандмауэра.

Тема 11 Безопасность операционной системы

Защита операционной системы: удаление ненужного ПО и служб, замена учетных записей по умолчанию, использование принципа наименьший привилегий, регулярные обновления, ведение журнала и аудит. Вредоносное ПО: меры защиты. Инструменты безопасности операционной системы: сканеры, оценка уязвимостей, фреймворки эксплойтов.

Тема 12 Безопасность мобильных устройств, встроенных устройств и интернета вещей

Безопасность мобильных устройств: защита устройств, основные проблемы безопасности. Безопасность встроенных устройств: определение встроенных устройств, области применения, проблемы безопасности. Безопасность интернета вещей: определение IoT, проблемы безопасности.

Тема 13 Безопасность приложений

Уязвимости разработки программного обеспечения: переполнение буфера, атаки проверки ввода, аутентификации, авторизации, криптографические атаки. Веб-безопасность: атаки на стороне сервера, атаки на стороне клиента. Безопасность баз данных: проблемы протокола, доступ без аутентификации, выполнение произвольного кода, повышение уровня привилегий. Инструменты безопасности приложений: снифферы, инструменты анализа, фаззеры.

Тема 14 Оценка безопасности

Оценка уязвимости: отображение и обнаружение, сканирование, основные технологические вызовы. Тестирование на проникновение: понятие, цели, процесс, классификация, технологические вызовы. Реалистичное тестирование, определение инсайдерских атак, экономическая эффективность разработки системы безопасности и ее совершенствования.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР (дист.)	Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное			
1	2	3	4	5	6	7		8	9
1	Введение в информационную безопасность	2							Собеседование, разбор кейсов
2	Идентификация и аутентификация	2			4				Письменный отчет по практической работе №1, разбор кейсов
3	Контроль доступа. Внедрение и основные модели	2							Собеседование
4	Отчетность и аудит	2			4			2	Отчет по практической работе №2 с устной защитой, контрольная работа
5	Криптография	2			4				Письменный отчет по практической работе №3, электронный практикум
6	Соответствие требованиям, законодательство и нормативные положения	2							Разбор кейсов
7	Операционная безопасность	2			4			2	Письменный отчет по практической работе №4, контрольная работа

8	Человеческий фактор в информационной безопасности	2			4				Письменный отчет по практической работе №5, электронный практикум
9	Физическая безопасность	2							Собеседование
10	Сетевая безопасность	2			4				Письменный отчет по практической работе №6, электронный практикум
11	Безопасность операционной системы	2							Собеседование
12	Безопасность мобильных устройств, встроенных устройств и интернета вещей	2			4				Письменный отчет по практической работе №7, электронный практикум
13	Безопасность приложений	2			2			2	Отчет по практической работе №8 с устной защитой, собеседование, контрольная работа
14	Оценка безопасности	2			2				Отчет по практической работе №8 с устной защитой, электронный тест
	Итого	28			32			6	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Джейсон, А. Защита данных. От авторизации до аудита / А. Джейсон. – СПб. : Питер, 2021. – 272 с.

2. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы /В.Олифер, Н.Олифер. СПб: Питер, 2016. – 991 с.

3. Нестеров, С. А. Информационная безопасность. – М. : Юрайт, 2016. – 321 с. 6. Гришина, Н.В. Информационная безопасность предприятия. – М. : Форум : ИНФРА-М, 2016. – 238 с.

4. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах. – М. : Форум : Инфра-М, 2016. – 591 с.

5. Баранова, Е. К. Информационная безопасность и защита информации : Учебное пособие / Е. К. Баранова, А. В. Бабач. – 3-е изд. – Москва : ИЦ РИОР, НИЦ ИНФРА-М, 2016. – 322 с.

Перечень дополнительной литературы

1. Цуканова, О. А. Экономика защиты информации : Учебное пособие / О. А. Цуканова, С. Б. Смирнов. – Санкт-Петербург: Университет ИТМО, 2014. – 90 с.

2. Некраха, А. В. Организация конфиденциального делопроизводства и защита информации : Учебное пособие / А. В. Некраха, Г. А. Шевцова. – Москва: Академический Проект, 2016. – 224 с.

3. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. – Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. – 113 с.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Для диагностики компетенций используются следующие формы: устная; письменная; устно-письменная; техническая. К устной форме диагностики компетенций относятся: собеседования. К письменной форме диагностики компетенций относятся: контрольные работы, письменные отчеты по лабораторным. К устно-письменной форме диагностики компетенций относятся: отчеты по лабораторным с их устной защитой, кейсы. К технической форме диагностики компетенций относятся: электронные тесты, электронные практикумы.

Оценка работы на практических занятиях формируется на основе следующих критериев: умение воспроизвести выполнение заданий, понимание практической применимости результатов работы, качество выполнение лабораторной проектной работы, качество анализа и интерпретации кейсов.

Формой текущей аттестации по дисциплине «Информационная безопасность» учебным планом предусмотрен зачет.

При формировании итоговой отметки используется рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний и текущей аттестации в итоговую отметку:

Формирование отметки за текущую успеваемость:

- выполнение практических работ №1–8 – 40%;
- выполнение контрольных работ – 60%.

Итоговая отметка по дисциплине рассчитывается на основе отметки текущей успеваемости (рейтинговой системы оценки знаний) и зачетной отметки с учетом их весовых коэффициентов. Вес отметки по текущей успеваемости составляет 40 %, зачетной отметки – 60 %.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Тема 4 Отчетность и аудит (2 ч.)

1. В чем заключается отличие между авторизацией и отчетностью.
2. Дайте определение понятию «неоспоримость».
3. Приведите не менее пяти примеров потенциальных объектов проверки.
4. Аргументируйте необходимость отчетности при работе с конфиденциальными данными

5. Объясните, в чем заключается разница между оценкой уязвимости и тестированием на проникновение.
6. Пусть есть среда, содержащая серверы, которые обрабатывают конфиденциальные данные клиентов, некоторые из них доступны в интернете. Что можно выполнить — оценку уязвимости, тест на проникновение или и то и другое? Почему?
Форма контроля – контрольная работа

Тема 7 Операционная безопасность (2 ч.)
1. Дайте определение первого закона OPSEC.
2. В чем заключается функция IOSS?
3. Объясните разницу между оценкой угроз и оценкой уязвимостей в процессе обеспечения операционной безопасности.
4. Для чего нужна классификация информации?
5. Как вы считаете, можно ли считать работу завершенной при условии окончания процесса обеспечения операционной безопасности? Аргументируйте свой ответ.
6. Дайте определение конкурентной контрразведке.
Форма контроля – контрольная работа

Тема 13 Безопасность приложений (2 ч.)
1. Приведите пример состояния гонки.
2. Что делает инструмент Burp Suite и в какой ситуации его можно было бы использовать?
3. Перечислите основные категории веб-безопасности и охарактеризуйте их.
4. Что такое подделка межсайтового запроса и как можно предотвратить эту атаку?
5. Как можно использовать сниффер для повышения безопасности приложений?
6. Как можно использовать сниффер для повышения безопасности приложений?
Форма контроля – контрольная работа

Примерная тематика практических занятий

1. Разработка политики информационной безопасности организации
2. Оценка риска и моделирование угроз информационное безопасности
3. Симметричные алгоритмы, шифры перестановки
4. Подстановочные шифры, криптоанализ
5. Шифрование с открытым ключом
6. Контроль целостности данных. Электронная цифровая подпись
7. Шифрование открытого текста на основе эллиптических кривых
8. Организация защиты ресурсов в ИС организации

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используются следующие инновационные подходы и методы.

1. ***Практико-ориентированный подход,*** который предполагает***:***

– освоение содержание образования через решения практических задач;

– приобретение навыков эффективного выполнения разных видов профессиональной деятельности;

– ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;

– использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

2. ***Метод анализа конкретных ситуаций (кейс-метод),*** который предполагает***:***

– приобретение студентом знаний и умений для решения практических задач;

– анализ ситуации, используя профессиональные знания, собственный опыт, дополнительную литературу и иные источники.

3. ***Метод учебной дискуссии,*** который предполагает участие студентов в целенаправленном обмене мнениями, идеями для предъявления и/или согласования существующих позиций по определенной проблеме.

Использование метода обеспечивает появление нового уровня понимания изучаемой темы, применение знаний (теорий, концепций) при решении проблем, определение способов их решения.

4. ***Методы и приемы развития критического мышления,*** которые представляют собой систему, формирующую навыки работы с информацией в процессе чтения и письма; понимании информации как отправного, а не конечного пункта критического мышления.

Методические рекомендации по организации самостоятельной работы обучающихся

При изучении учебной дисциплины используются следующие формы самостоятельной работы:

– выполнение заданий, выдаваемых на практических занятиях;
– изучение материала, выносимого на самостоятельную проработку;
– подготовка к практическим занятиям;
– подготовка к зачету

Примерные варианты тестовых вопросов к зачету

1. Группа компьютеров, объединенных в сеть и используемых хакерами для кражи информации, называется …

A) Ботнет
B) Руткит
C) DDoS
D) Операционная система

2. Если для доступа к общедоступной сети Wi-Fi (например, в аэропорту или кафе) требуется пароль, безопасно ли использовать эту сеть для таких чувствительных видов деятельности, как онлайн-банкинг?

A) Да, безопасно
B) Нет, небезопасно
C) Безопасно только во время осуществления чувствительных видов деятельности за других людей
D) Ничто из вышеперечисленного

3. Злоумышленники получают доступ к чьему-либо компьютеру и шифруют личные файлы и данные пользователя. Пользователи не могут получить доступ к этим данным, если они не заплатят преступникам за расшифровку файлов. Данная практика называется …

A) Botnet
B) Ransomware
C) Driving
D) Spam
E) Ничто из вышеперечисленного

4. Какие риски кибербезопасности можно минимизировать с помощью виртуальной частной сети (VPN)?

A) Использование небезопасных Wi-Fi сетей
B) Кейлоггинг
C) Деанонимизация операторами сети
D) Фишинговые атаки

5. Какой из следующих паролей является наиболее безопасным?

A) Boat123
B) WTh!5Z
C) into*48
D) 123456

6. На каком этапе этического хакинга мы получаем информацию о ПО, логины сотрудников, директории, информацию о политике компании и т.д.?

A) Разведка и футпринтинг
B) Сканирование и перечисление
C) Получение доступа
D) Удержание доступа

E) Заметение следов

7. Основными компонентами атаки являются:
A) Безопасность, функциональность, юзабилити
B) Разведка, хакинг, удержание доступа
C) Мотив, метод, уязвимость
D) Злоумышленник, жертва, устройство

8. Отключение функции GPS на вашем смартфоне предотвращает отслеживание местоположения вашего телефона.
A) Да
B) Нет

9. Что из нижеперечисленного является примером «фишинговой» атаки?
A) Отправка кому-либо электронного письма, содержащего вредоносную ссылку, замаскированную под электронное письмо от знакомого человека
B) Создание поддельного сайта, который выглядит почти идентичным реальному сайту, чтобы обманом заставить пользователей вводить свои регистрационные данные
C) Отправка кому-либо текстового сообщения, содержащего вредоносную ссылку, замаскированную под уведомление о том, что человек выиграл конкурс
D) Все вышеперечисленное

10. Что означает «https://» в начале URL-адреса, в отличие от «http://»?
A) Сайт имеет высокий рейтинг
B) Информация, введенная на сайт, зашифрована
C) Сайт обновлен до самой последней доступной версии
D) Определенные браузеры не поддерживают отображение данного сайта
E) Ничто из вышеперечисленного

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Корпоративные информационные системы	Цифровой экономики	Изменений в учебной программе не требуется	29.06.2022, протокол № 10

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры цифровой экономики (протокол № ____ от _____ 202_ г.)

Заведующий кафедрой
к.э.н., доцент _____ И.А. Карачун

УТВЕРЖДАЮ
Декан факультета
к.ф.-м.н., доцент _____ А.А. Королева