БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе
и образовательным инновациям
_____ О.Г. Прохоренко
«30» июня 2023 г.

Регистрационный № УД-12081 /уч.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-96 01 02 Экономическая безопасность

2023 г.

Учебная программа составлена на основе ОСВО 1-96 01 02-2021, учебных планов Р 96-1-203/уч. от 22.03.2022 г., Р 96-1-001/уч. от 25.05.2021 г.,

СОСТАВИТЕЛЬ:
В. А. Макаревич, старший 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 № 11 от 30.06.2023);
Научно-методическим Советом БГУ
(протокол № 9 от 29.06.2023)

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.

Учебная дисциплина «Информационная безопасность» относится к модулю «Основы экономической безопасности» государственного компонента.

Требования к компетенциям

Освоение учебной дисциплины «Информационная безопасность» должно обеспечить формирование следующих компетенций:

Базовые профессиональные компетенции:

БПК-10. Использовать информационные системы и технологии, проводить информационно-поисковую работу для обеспечения экономической безопасности.

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 – 132 часа, в том числе 68 аудиторных часа, из них: лекции – 34 часов, практические занятия – 34 часа.

Трудоемкость учебной дисциплины составляет 3 зачетных единицы.

Форма текущей аттестации – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1 Введение в информационную безопасность
Основные термины, цели защиты, слабые места и угрозы, типы атак и атакующих, компьютерная криминалистика, правила безопасности и многосторонняя безопасность, новые угрозы.

Тема 2 Угрозы
Вредоносное программное обеспечение, переполнение буфера, компьютерные вирусы, черви, троянский конь (троян), бот-нет, спам, мобильные приложения, новые виды угроз: атаки Meltdown и Spectre.

Тема 3 Проблемы безопасности интернет-протоколов
Введение в проблему безопасности интернет-протоколов, протокол IP, протокол TCP, проблемы безопасности IP, маршрутизационные атаки, проблемы безопасности ICMP, проблемы безопасности ARP, проблемы безопасности IPv6, проблемы безопасности UDP и TCP, DNS, NFS, электронная почта, File Transfer Protocol, веб-приложения, динамические веб-сайты, куки, проблемы безопасности HTML5.

Тема 4 Построение системы безопасности. Критерии оценки
Общие принципы создания IT-систем, структурный анализ, определение потребности в защите, анализ угроз, анализ рисков, тесты на атаку, архитектура безопасности, базовые функции безопасности, жизненный цикл безопасной разработки (Security Development Lifecycle). Моделирование угроз на основе универсального шаблона.
Введение в проблематику критериев оценки, TCSEC — Trusted Computer System Evaluation Criteria, ITSEC — Information Technology Security Evaluation Criteria, Common Criteria for Information Technology Security Evaluation.

Тема 5 Модели безопасности
Объекты и субъекты, права доступа, виды ограничения прав доступа, стратегии безопасности, матричная модель доступа, модели, основанные на ролях, модель «Китайская стена», модель Белла — Лападулы.

Тема 6 Технологии работы с ключами
Создание ключей, техники создания ключей, хранение и уничтожение ключей, обмен ключами, иерархия ключей, наивный протокол обмена ключами, симметричные алгоритмы обмена ключами, асимметричные протоколы обмена ключами, принципы разработки протоколов обмена ключами, восстановление ключей.

Тема 7 Аутентификация на основе знания
Аутентификация на основе паролей, использование одноразовых паролей для аутентификации (метод S/Key), методы «вызов — ответ».

Тема 8 Аутентификация на основе обладания предметом. Биометрическая аутентификация

Смарт-карты, универсальная аутентификация по двум факторам, Trusted Computing, физически неклонируемые функции, общие сведения о биометрических технологиях, особенности процесса биометрической аутентификации.

Тема 9 Особенности аутентификации в распределенных системах

Протокол RADIUS, AAA-архитектура, технология Blockchain, биткойн — практическая реализация блокчейна.

Тема 10 Основы криптографической защиты информации

Шифр Цезаря, шифр перестановки, шифр перестановки «сцитала», диск и линейка Энея, квадрат Полибия, тюремный шифр, магические квадраты, шифр Аве Мария, таблица Тритемия, шифр Бэкона, шифр Порты, шифр Кардано, шифр Ришелье, симметричное и асимметричное шифрование, безопасность методов шифрования.

Тема 11 Современные криптографические алгоритмы

Блочные шифры, режимы шифрования, поточные шифры, понятие и свойства идеального шифра, асимметричные шифры. RSA-алгоритм, шифр Рабина, обмен ключами Диффи — Хеллмана, алгоритм Эль-Гамаля.

Тема 12 Электронная цифровая подпись

Общие сведения об электронной цифровой подписи, одноразовая подпись Лемпорта — Диффи, подпись RSA, подпись Эль-Гамаля.

Тема 13 Безопасность сетей

Технология межсетевого экрана (брандмауэра, файрвола), пакетные фильтры, прокси межсетевые экраны, фильтры приложений, варианты архитектуры, использующей межсетевые экраны, протоколы безопасной коммуникации, виртуальная частная сеть, IPSec, протокол TLS/SSL, DNSSEC, электронная почта, PGP.

Тема 14 Безопасность мобильной и беспроводной связи

GSM, GPRS, UMTS, LTE и SAE, 5G и будущее сотовой связи, WLAN, Bluetooth, ZigBee.

Тема 15 Инженерно-техническая защита информации

Особая важность инженерно-технической защиты, направления и методы инженерно-технической защиты информации, средства технической охраны, акустические каналы утечки информации, оптические каналы утечки информации, радиоэлектронные каналы утечки информации.

Тема 16 Правовые основы информационной безопасности

Основные понятия и определения. Управление, социология, психология, право, организация в защите данных от несанкционированного использования. Государственный стандарт Республики Беларусь 50922-2006 «Защита информации. Основные термины и определения». Виды информации в соответствии с Законом Республики Беларусь № 455-З «Об информации, информатизации и защите информации». Концепция национальной безопасности Республики Беларусь. Концепция информационной безопасности Республики Беларусь.

Тема 17 Управление IT-проектом как эффективный способ организации действий по повышению уровня информационной безопасности

Понятие проекта, виды и фазы проектов, управление проектами как специфический вид менеджмента, типичные проблемы реализации проектов, проект от определения до завершения.

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	2						Собеседование, разбор кейсов
2	Угрозы	2	2						Письменный отчет по практической работе №1, разбор кейсов
3	Проблемы безопасности интернет-протоколов	2	2						Собеседование. Устная защита отчета по практической работе №2
4	Построение системы безопасности. Критерии оценки	2	2						Отчет по практической работе №3 с устной защитой, контрольная работа
5	Модели безопасности	2	2						Письменный отчет по практической работе №4, собеседование
6	Технологии работы с ключами	2	2						Отчет по практической работе №5 с устной защитой
7	Аутентификация на основе знания	2	2						Отчет по практической работе №6 с устной

									защитой, контрольная работа
8	Аутентификация на основе обладания предметом. Биометрическая аутентификация	2	2						Письменный отчет по практической работе №7
9	Особенности аутентификации в распределенных системах	2	2						Электронный практикум
10	Основы криптографической защиты информации	2	2						Электронный практикум
11	Современные криптографические алгоритмы	2	2						Собеседование
12	Электронная цифровая подпись	2	2						Письменный отчет по практической работе №10
13	Безопасность сетей	2	2						Отчет по практической работе №11 с устной защитой, собеседование, контрольная работа
14	Безопасность мобильной и беспроводной связи	2	2						Отчет по практической работе №12 с устной защитой, собеседование
15	Инженерно-техническая защита информации	2	2						Отчет по практической работе №13 с устной защитой
16	Правовые основы информационной безопасности	2	2						Отчет по практической работе №14 с устной защитой
17	Управление IT-проектом как эффективный способ организации действий по повышению уровня информационной безопасности	2	2						Электронный тест, собеседование
	Итого	34	34						

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Сычев Ю. Н. Защита информации и информационная безопасность : Учебное пособие / Российский экономический университет им. Г.В. Плеханова. – 1. – Москва : ООО "Научно-издательский центр ИНФРА-М", 2023. – 201 с.

2. Нестеров С. А. Основы информационной безопасности : учебное пособие / Нестеров С. А. – 5-е изд., стер. – Санкт-Петербург : Лань, 2022. – 324 с.

3. Мандрица И. В. Управление проектами по информационной безопасности и экономика защиты информации. Часть 1 : учебник для вузов / Мандрица И. В.,Петренко В. И.,Мандрица О. В. – Санкт-Петербург : Лань, 2023. – 124 с.

Перечень дополнительной литературы

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

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

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

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

5. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. – Москва : Издательство Юрайт, 2022. – 259 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 экзамен.

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 %.

Примерная тематика практических занятий

1. Проектное задание: моделирование угроз.
2. Проектное задание: интернет-протоколы.
3. Проектное задание: анализ системы безопасности.
4. Проектное задание: классификация IT-системы организации.
5. Проектное задание: разработка модели безопасности.
6. Проектное задание: работа с ключами в организации.
7. Проектное задание: технологии аутентификации.
8. Симметричные алгоритмы, шифры перестановки.

9. Подстановочные шифры, криптоанализ.

10. Проектное задание: технологии безопасности сетей.

11. Проектное задание: безопасность беспроводных сетей.

12. Проектное задание: инженерно-техническая защита информации.

13. Проектное задание: стандарты в области защиты информации.

14. Проектное задание: разработка проекта в сфере информационной безопасности.

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 экзамену

Примерные варианты тестовых вопросов к экзамену

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	30.06.2023, протокол № 11

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