АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ»
«УНИВЕРСИТЕТ ЭКОНОМИКИ И УПРАВЛЕНИЯ»
Факультет экономики, управления и юриспруденции
Кафедра «Управление и бизнес-информатика»

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_________ Е.В. Бебешко
«31» марта 2023 г.

Рабочая программа дисциплины

Информационная безопасность и защита информации

Направление подготовки
38.03.05 Бизнес-информатика

Профиль
Специалист по информационным системам и технологиям

Квалификация выпускника
Бакалавр

Для всех
форм обучения

Симферополь 2023

АННОТАЦИЯ	
Индекс дисциплины по учебному плану	Наименование дисциплины
Б1.В.10	**Информационная безопасность и защита информации**
Цель изучения дисциплины	формирование у обучающихся навыков, связанных с обеспечением защиты информации; при решении задач, связанных с обеспечением информационной безопасности объектов информатизации; представлений об основах информационной безопасности, принципах и методах противодействия несанкционированному информационному воздействию.
Место дисциплины в структуре ОПОП	Дисциплина относится к части, формируемой участниками образовательных отношений блока 1. «Дисциплины (модули)» программы бакалавриата
Компетенции, формируемые в результате освоения дисциплины	ПК-3
Содержание дисциплины	Тема 1. Общие вопросы информационной безопасности Тема 2. Государственная система информационной безопасности Тема 3. Угрозы безопасности Тема 4. Теоретические основы методов защиты информационных систем Тема 5. Методы защиты средств вычислительной техники Тема 6. Основы криптографии Тема 7. Архитектура защищенных экономических систем Тема 8. Алгоритмы безопасности в компьютерных сетях
Общая трудоемкость дисциплины	Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часа)
Форма промежуточной аттестации	Зачет с оценкой

Содержание

1. Цель и перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы бакалавриата

Цель изучения дисциплины «Информационная безопасность и защита информации» является формирование у обучающихся навыков, связанных с обеспечением защиты информации; при решении задач, связанных с обеспечением информационной безопасности объектов информатизации; представлений об основах информационной безопасности, принципах и методах противодействия несанкционированному информационному воздействию.

В результате освоения ОПОП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине:

Коды компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения по дисциплине
ПК-3	Способен управлять архитектурой и ИТ-инфраструктурой предприятия, обеспечивать надлежащий уровень информационной безопасности	ПК-3.1. **Знает** методы анализа архитектуры, ИТ-инфраструктуры предприятия, нормативную документацию, регулирующую отношения в области информационной безопасности; ПК-3.2. **Умеет** моделировать архитектуру, ИТ-инфраструктуру предприятия, настраивать политики безопасности; ПК-3.3. **Владеет** навыками управления архитектурой и ИТ-инфраструктурой предприятия, обеспечения надлежащего уровня информационной безопасности.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина Б1.В.10 «Информационная безопасность и защита информации» относится к части, формируемой участниками образовательных отношений блока 1учебного плана ОПОП бакалавриата по направлению подготовки 38.03.05 Бизнес-информатика. Дисциплина «Информационная безопасность и защита информации» изучается обучающимися очной формы обучения в 8 семестре, очно-заочной формы обучения – в 8 семестре.

При изучении данной дисциплины обучающийся использует знания, умения и навыки, которые сформированы в процессе изучения предшествующих дисциплин: «Информационные технологии в профессиональной деятельности», «Компьютерные сети», «Стандартизация, сертификация и техническое документоведение».

Знания, умения и навыки, полученные при изучении дисциплины «Информационная безопасность и защита информации», будут необходимы для углубленного и осмысленного восприятия дисциплин: «Основы цифровой экономики», «Корпоративные информационные системы», в производственной практике, подготовке выпускной квалификационной работы.

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 4 зачетных единицы (з.е.), 144 академических часа.

3.1. Объём дисциплины по видам учебных занятий (в часах)

Для очной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	144
Контактная работа	44
Аудиторная работа(всего):	44
Лекции	16
Семинары, практические занятия	28
Самостоятельная работа обучающихся (всего)	100
Курсовая работа	-
Зачет с оценкой	+
Экзамен	-

Для очно-заочной формы обучения

Общая трудоёмкость дисциплины составляет 4 зачётных единицы 144 часа

Объём дисциплины	Всего часов
Общая трудоемкость дисциплины	144
Контактная работа	34
Аудиторная работа(всего):	34
Лекции	12
Семинары, практические занятия	22
Самостоятельная работа обучающихся (всего)	110
Курсовая работа	-
Зачет с оценкой	+
Экзамен	-

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ темы	Наименование темы	Всего		Количество часов					
				Контактная работа				Внеаудит. работа	
				Лекции		Практические		Самост. работа	
		ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО	ОФО	ОЗФО
1.	Общие вопросы информационной безопасности	14	14	2	2	2	2	10	10
2.	Государственная система информационной безопасности	18	18	2	2	2	2	14	14
3.	Угрозы безопасности	14	14	2	2	2	2	10	10
4.	Теоретические основы методов защиты информационных систем	22	22	2	2	4	4	16	16
5.	Методы защиты средств вычислительной техники	20	20	2		4	4	14	16
6.	Основы криптографии	24	24	2	2	6	4	16	18
7.	Архитектура защищенных экономических систем	16	16	2	2	4	2	10	12
8.	Алгоритмы безопасности в компьютерных сетях	16	16	2		4	2	10	14
	Всего по дисциплине	**144**	**144**	**16**	**12**	**28**	**22**	**100**	**110**
	Контроль	-	-						
	Итого	**144**	**144**						

4.2. Содержание дисциплины, структурированное по темам(разделам)

Тема 1. Общие вопросы информационной безопасности

Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.

Тема 2. Государственная система информационной безопасности

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения

информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

Тема 3. Угрозы безопасности

Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

Тема 4. Теоретические основы методов защиты информационных систем

Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-Ла-Падулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.

Тема 5. Методы защиты средств вычислительной техники

Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

Тема 6. Основы криптографии

Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Сжатие информации.

Тема 7. Архитектура защищенных экономических систем

Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации. Ядро и ресурсы средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем.

Тема 8. Алгоритмы безопасности в компьютерных сетях

Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.

4.3.Содержание практических занятий (очная форма обучения)

Практическое занятие № 1. Общие вопросы информационной безопасности. (2 часа) 1. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. 2. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная. 3.Выполнение практических заданий.
Практическое занятие № 2. Государственная система информационной

безопасности (2 часа)

1. Доктрина информационной безопасности Российской Федерации.
2. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации.
3. Выполнение практических заданий.

Практическое занятие № 3. Угрозы безопасности (2 часа).

1. Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз.
2. Классы каналов несанкционированного получения информации.
3. Выполнение практических заданий.

Практическое занятие № 4-5. Модели безопасности и их применение (4 часа)

1. Формальные модели безопасности.
2. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-Ла-Падулы.
3. Выполнение практических заданий.

Практическое занятие 6-7 Методы защиты средств вычислительной техники. (4 часа)

1. Аппаратные и программные средства для защиты компьютерных систем от НСД.
2. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.
3. Выполнение практических заданий.

Практическое занятие 8-9. Методологические основы бизнес-информатики (4 часа).

1. Симметричное и асимметричное шифрование. Алгоритмы шифрования.
2. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. Хеширование. Имитовставки. Криптографические генераторы случайных чисел..
3. Выполнение практических заданий.

Практическое занятие 10. Способы распространения ключей (2 часа).

1. Способы распространения ключей. Обеспечиваемая шифром степень защиты.
2. Криптоанализ и атаки на криптосистемы. Сжатие информации.
3. Выполнение практических заданий.

Практическое занятие 11-12. Основные технологии построения защищенных экономических информационных систем. (4 часа).

1. Основные технологии построения защищенных экономических информационных систем. Функции защиты информации. Классы задач защиты информации.
2. Архитектура систем защиты информации. Ядро и ресурсы средств защиты информации. Стратегии защиты информации. Особенности экономических информационных систем.
3. Выполнение практических заданий.

Практическое занятие 13-14. Алгоритмы безопасности в компьютерных сетях. . (4 часа).

1. Межсетевые экраны. Проектирование МЭ. Снифферы. Эксплоиты.
2. Атаки на сервера. Атаки на рабочие станции. Атака типа «отказ в обслуживании». Протоколирование. Сетевые защищенные протоколы.
3. Выполнение практических заданий.

4.4. Содержание самостоятельной работы

Тема 1. Общие вопросы информационной безопасности Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
Тема 2. Государственная система информационной безопасности Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
Тема 3. Угрозы безопасности Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
Тема 4. Теоретические основы методов защиты информационных систем Модель распространения прав доступа Take-Grant. Мандатная модель Белла-Ла-Падулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.
Тема 5. Методы защиты средств вычислительной техники Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.
Тема 6. Основы криптографии Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Сжатие информации.
Тема 7. Архитектура защищенных экономических систем Стратегии защиты информации. Особенности экономических информационных систем.
Тема 8. Алгоритмы безопасности в компьютерных сетях Протоколирование. Сетевые защищенные протоколы.

5. Контроль качества освоения дисциплины

Текущий контроль и промежуточная аттестация осуществляются в соответствии с «Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся в Автономной некоммерческой организации «Образовательная организация высшего образования» «Университет экономики и управления».

Вид промежуточной аттестации – зачет с оценкой. Форма проведения промежуточной аттестации – письменный зачет с оценкой.

Фонд оценочных средств по дисциплине приведен в приложении к РПД.

6. Учебно-методическое обеспечение дисциплины

1. Терминологический словарь по предметам кафедры «Бизнес-информатика» / составители Я. А. Донченко [и др.]. — Симферополь : Университет экономики и управления, 2020. — 240 c. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/108063.html (дата обращения: 03.03.2023). — Режим доступа: для авторизир. пользователей.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная

1. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 03.03.2023). — Режим доступа: для авторизир. пользователей.

2. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 c. — ISBN 978-5-4487-0585-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/86938.html (дата обращения: 03.03.2023). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/86938

3. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 c. — ISBN 978-5-4497-1653-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/120489.html (дата обращения: 03.03.2023). — Режим доступа: для авторизир. пользователей.

б) дополнительная

1. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 c. — ISBN 978-5-4497-0338-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89453.html (дата обращения: 03.03.2023). — Режим доступа: для авторизир. пользователей.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Информационно-правовой портал «Гарант»: официальный сайт. – URL: http://www.garant.ru – Текст: электронный.
2. Цифровой образовательный ресурс «IPRsmart»: официальный сайт. – URL: http:// www.iprbookshop.ru/ – Текст: электронный.
3. Научная электронная библиотека «КиберЛенинка»: официальный сайт. – URL: https://cyberleninka.ru/ – Текст: электронный.
4. Российский интернет-портал и аналитическое агентство TAdviser: официальный сайт. – URL: https://www.tadviser.ru/ – Текст: электронный.
5. Научный журнал «Вопросы кибербезопасности»: официальный сайт. – URL: http://cyberrus.com – Текст: электронный.

9. Методические указания для обучающихся по освоению дисциплины

При проведений лекций, семинарских (практических) занятий, самостоятельной работе обучающихся применяются интерактивные формы проведения занятий с целью погружения обучающихся в реальную атмосферу профессионального сотрудничества по разрешению проблем, оптимальной выработки навыков и качеств будущего специалиста. Интерактивные формы проведения занятий предполагают обучение в сотрудничестве. Все участники образовательного процесса (преподаватель и обучающиеся) взаимодействуют друг с другом, обмениваются информацией, совместно решают проблемы, моделируют ситуацию.

В учебном процессе используются интерактивные формы занятий:

- творческое задание. Выполнение творческих заданий требует от обучающегося воспроизведение полученной ранее информации в форме, определяемой преподавателем, и требующей творческого подхода;

- групповое обсуждение. Групповое обсуждение кого-либо вопроса направлено на достижении лучшего взаимопонимания и способствует лучшему усвоению изучаемого материала.

В ходе освоения дисциплины при проведении контактных занятий используются следующие формы обучения, способствующие формированию компетенций: лекции-дискуссии; кейс-метод; решение задач; ситуационный анализ; обсуждение рефератов и докладов; разработка групповых проектов; встречи с представителями государственных и общественных организаций.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

В процессе лекционных и практических занятий используется следующее программное обеспечение:

*программы, обеспечивающие доступ в сеть «Интернет» (например, «MicrosoftEdge», «GoogleChrome»);

*программы, демонстрации видео материалов (например, проигрыватель «WindowsMediaPlayer»);

*текстовые редакторы и процессоры (например, «Блокнот», «MicrosoftOfficeWord»);

*программы для демонстрации и создания презентаций (например, «MicrosoftPowerPoint»).

11. Описание материально-технического обеспечения, необходимого для осуществления образовательного процесса по дисциплине

Для преподавания дисциплины требуется специальные материально-технические средства (компьютерные классы и т.п.). Во время лекционных занятий, которые проводятся в большой аудитории, используется проектор для демонстрации слайдов, схем, таблиц и прочего материала, мультимедийные проекторы Epson, BenqViewSonic; экраны для проекторов; ноутбуки Asus, Lenovo, микрофоны.