Министерство сельского хозяйства Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный аграрный университет»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00F5277CD9C866ACF46E54698E7375A77F
Владелец: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ"
Действителен: с 14.03.2023 до 06.06.2024

УТВЕРЖДАЮ
Врио проректора по учебной,
воспитательной работе и
молодежной политике
доцент Ю.З. Кирова

«19» мая 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление информационными системами в сфере экономической безопасности

Специальность: ***38.05.01 Экономическая безопасность***

Специализация: ***Экономико-правовое обеспечение экономической безопасности***

Название кафедры: ***Менеджмент и маркетинг***

Квалификация: ***экономист***

Форма обучения: ***очная, заочная***

Кинель 2022

1 ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Управление информационными системами в сфере экономической безопасности» является формирование навыков организации системы управления информационной безопасностью в профессиональной деятельности.

Для достижения поставленной цели при освоении дисциплины решаются следующие *задачи*:

– выработка навыков организации и методологии обеспечения информационной безопасности в коммерческих организациях и организациях банковской системы РФ;

- создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях в управлении информационной безопасностью в коммерческих организациях и организациях банковской системы РФ;

- развитие способностей по использованию существующей системы управления информационной безопасности.

2 МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина Б1.В.16 «Управление информационными системами в сфере экономической безопасности» относится к дисциплинам части, формируемой участниками образовательных отношений, блока 1 «Дисциплины (модули)» учебного плана.

Дисциплина изучается в 7 семестре на IV курсе очной и заочной форм обучения.

3 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ / ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ЗАВЕРШЕНИИ ОСВОЕНИЯ ПРОГРАММЫ ДИСЦИПЛИНЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций (в соответствии с ФГОС ВО и требованиями к результатам освоения ОПОП).

Код компетенции	Результаты освоения ОПОП (Содержание компетенций)	Перечень планируемых результатов обучения по дисциплине
ПК-3	Способен реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать и использовать в интересах выявления рисков, локализации и нейтрализации угроз экономической безопасности, пресечения и расследования преступлений и иных правонарушений в сфере экономики	ИД-1/ПК-3 Знает законодательство, нормативные правовые акты и правила внутреннего распорядка в целях экономической безопасности, перечень и признаки экономических преступлений в отношении хозяйствующего субъекта ИД-2/ПК-3 Определяет источники информации для проведения финансового расследования в целях экономической безопасности организации ИД-3/ПК-3 Подготавливает аналитические материалы о выявлении в организации операций (сделок), имеющих признаки неправомерности и необычности ИД-4/ПК-3 Выполняет экспертные процедуры с использованием современных подходов и методов, информационных технологий и программных продуктов

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

для очной формы обучения

Вид учебной работы		Трудоемкость дисциплины		Семестры (кол-во недель в семестре)
		Всего часов	Объем контактной работы	7 (18)
Аудиторная контактная работа (всего)		36	36	36
в том числе:	Лекции	18	18	18
	Лабораторные работы	18	18	18
Самостоятельная работа обучающегося (всего), в том числе:		72	0,25	72
СР в семестре:	Изучение вопросов, выносимых на самостоятельное изучение	48		48
	Подготовка к лабораторным работам	18		18
СР в сессию:	зачет	6	0,25	6
Вид промежуточной аттестации (зачет, экзамен)		зачет		зачет
Общая трудоемкость, ч.		108	36,25	108
Общая трудоемкость, зачетные единицы		3		3

для заочной формы обучения

Вид учебной работы		Трудоемкость дисциплины		Семестры (кол-во недель в семестре)
		Всего часов	Объем контактной работы	7 (3)
Аудиторная контактная работа (всего)		12	12	12
в том числе:	Лекции	6	6	6
	Лабораторные работы	6	6	6
Самостоятельная работа обучающегося (всего), в том числе:		96	0,25	72
СР в семестре:	Изучение вопросов, выносимых на самостоятельное изучение	80		80
	Подготовка к лабораторным работам	12		12
СР в сессию:	зачет	4	0,25	4
Вид промежуточной аттестации (зачет, экзамен)		зачет		зачет
Общая трудоемкость, ч.		108	12,25	108
Общая трудоемкость, зачетные единицы		3		3

4.2 Тематический план лекционных занятий

для очной формы обучения

№ п/п	Тема лекционных занятий	Трудоемкость, ч.
1	Деятельность по обеспечению информационной безопасности.	2

2	Принципы, формы и методы деятельности по обеспечению информационной безопасности.	2
3	Информационная сущность бизнеса	2
4	Модель информационной безопасности бизнеса.	2
5	Модели непрерывного совершенствования и корпоративное управление.	2
6	Модели непрерывного совершенствования и международные стандарты.	2
7	Шаги реализации стандартной системы управления информационной безопасностью организации.	2
8	Формализованное представление угроз информационной безопасности от персонала.	2
9	Противодействие угрозам информационной безопасности от персонала.	2
Всего:		18

для заочной формы обучения

№ п/п	Тема лекционных занятий	Трудоемкость, ч.
1	Деятельность по обеспечению информационной безопасности.	2
2	Модель информационной безопасности бизнеса.	2
3	Шаги реализации стандартной системы управления информационной безопасностью организации.	2
Всего:		6

4.3 Тематический план практических занятий

Практические занятия учебным планом не предусмотрены

4.4 Тематический план лабораторных работ

для очной формы обучения

№ п/п	Темы лабораторных работ	Трудоемкость, ч.
1	Деятельность по обеспечению информационной безопасности.	2
2	Принципы, формы и методы деятельности по обеспечению информационной безопасности.	2
3	Информационная сущность бизнеса	2
4	Модель информационной безопасности бизнеса.	2
5	Модели непрерывного совершенствования и корпоративное управление.	2
6	Модели непрерывного совершенствования и международные стандарты.	2
7	Шаги реализации стандартной системы управления информационной безопасностью организации.	2
8	Формализованное представление угроз информационной безопасности от персонала.	2
9	Противодействие угрозам информационной безопасности от персонала.	2
Всего:		18

для заочной формы обучения

№ п/п	Темы лабораторных работ	Трудоемкость, ч.
1	Деятельность по обеспечению информационной безопасности.	2
2	Модель информационной безопасности бизнеса.	2
3	Шаги реализации стандартной системы управления информационной безопасностью организации.	2
Всего:		6

4.5 Самостоятельная работа

для очной формы обучения

Вид самостоятельной работы	Название (содержание работы)	Объем акад. часы
Изучение вопросов, выносимых на самостоятельное изучение	Самостоятельное изучение основной и дополнительной литературы, поиск и сбор информации по дисциплине в периодических печатных и интернет-изданиях, на официальных сайтов по вопросам: Характеристики делового общения. Значение языка жестов в деловом общении. Презентация как форма деловой коммуникации. Самопрезентация как форма деловой коммуникации. Метод записной книжки. Креативный вопросник. Комплименты в деловой коммуникации.	48
Подготовка к лабораторным работам	Изучение пройденного лекционного материала, выполнение домашнего задания	18
Зачет	Подготовка к зачету	6
ИТОГО		**72**

для заочной формы обучения

Вид самостоятельной работы	Название (содержание работы)	Объем акад. часы
Изучение вопросов, выносимых на самостоятельное изучение	Самостоятельное изучение основной и дополнительной литературы, поиск и сбор информации по дисциплине в периодических печатных и интернет-изданиях, на официальных сайтах по вопросам: Принципы, формы и методы деятельности по обеспечению информационной безопасности. Информационная сущность бизнеса. Модели непрерывного совершенствования и корпоративное управление. Модели непрерывного совершенствования и международные стандарты. Формализованное представление угроз информационной безопасности от персонала. Противодействие угрозам информационной безопасности от персонала.	80
Подготовка к практическим занятиям	Изучение пройденного лекционного материала, выполнение домашнего задания	12
Зачет	Подготовка к зачету	4
ИТОГО		**96**

5 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины необходимо начать с ознакомления с рабочей программой. Особое внимание следует обратить на вопросы, выносимые для самостоятельного изучения.

В тезисах лекций представлен теоретический материал по дисциплине согласно рабочему плану, в конце приведены вопросы для контроля знаний.

Изучая дисциплину необходимо равномерно распределять время на проработку лекций, самостоятельную работу по подготовке к лабораторным работам. Вопросы теоретического курса, вынесенные на самостоятельное изучение, наиболее целесообразно осваивать сразу после прочитанной лекции, составляя конспект по вопросу в тетради с лекционным материалом.

Если при изучении дисциплины у обучающихся возникают вопросы, то их можно обсудить на консультациях под руководством преподавателя.

При изучении темы «Противодействие угрозам информационной безопасности от персонала» студенту необходимо уделить особое внимание социальным аспектам данной проблемы.

При работе с литературой следует обратить внимание на источники основной и дополнительной литературы, приведенные в рабочей программе. Для большего представления о

дисциплине возможно ознакомление с периодическими изданиями последних лет, Интернет-источниками.

При подготовке к зачету особое внимание следует обратить на следующие моменты: зачет проводится в устной форме, при подготовке лучше структурировать и конспектировать материал. Положительная оценка на зачете ставится в случае правильного ответа на все вопросы билета.

6 ОСНОВНАЯ, ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И РЕСУРСЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ»:

6.1. Основная литература:

6.1.1. Канаков, А.Г Защита информации и интернет / А.Г Канаков. – Москва : ГАОУ ВПО МГИИТ имени Ю.А. Сенкевича, 2012. – 43 с. – Режим доступа: https://rucont.ru/efd/192851

6.1.2. Акмаров, П.Б. Кодирование и защита информации : учебное пособие / П.Б. Акмаров .– Ижевск : ФГБОУ ВО Ижевская ГСХА, 2016. – 136 с. – Режим доступа: https://rucont.ru/efd/363163

6.1.3. Белевская, Ю.А. Правовые основы информационной безопасности : учебник для вузов / А.П. Фисун, В.А. Минаев, А.В. Коськин, И.С. Константинов, В.А. Зернов, В.Т. Еременко, С.В. Дворянкин; Ю.А. Белевская. – Орел : ОрелГТУ, 2009. – 349 с. – URL: https://rucont.ru/efd/206354

6.2. Дополнительная литература:

6.2.1. Бышов, Н.В. Информационные технологии в экономике и управлении / Ф.А. Мусаев, В.В. Текучев, Л.В. Черкашина; Н.В. Бышов. – : [Б.и.], 2015. – 184 с. – Режим доступа: https://rucont.ru/efd/307046

6.2.2. Шашкова, И. Г. Информационные системы и технологии / В. С. Конкина, Е. И. Машкова; И. Г. Шашкова. – : [Б.и.], 2013. – 541 с. – Режим доступа: https://rucont.ru/efd/225944

6.2.3. Алексеев, А.П. Многоуровневая защита информации : монография / А.П. Алексеев. – Самара : ИУНЛ ПГУТИ, 2017. – 128 с. : ил. – Библиогр.: с. 124-126. – Режим доступа: https://rucont.ru/efd/641624

6.3. Программное обеспечение:

6.3.1. Microsoft Windows 7 Профессиональная 6.1.7601 Service Pack 1;
6.3.2. Microsoft Windows SL 8.1 RU AE OLP NL;
6.3.3. Microsoft Office стандартный 2013;
6.3.4. Microsoft Office Standard 2010;
6.3.5. Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition;
6.3.6. WinRAR:3.x: Standard License – educational –EXT;
6.3.7. 7 zip (свободный доступ).

6.4. Перечень информационно-справочных систем и профессиональных баз данных:

6.4.1. http://www.consultant.ru – Справочная правовая система «Консультант Плюс»;

6.4.2. http://www.garant.ru – Справочно-правовая система по законодательству Российской Федерации «Гарант»;

6.4.3. https://www.scopus.com/ – реферативная и справочная база данных рецензируемой литературы Scopus;

6.4.4. https://apps.webofknowledge.com – политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных Web of Science;

6.4.5. http://www.elibrary.ru/ – база данных Научной электронной библиотеки eLIBRARY.RU;

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

№ п/п	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	Учебная аудитория для проведения учебных занятий, оснащенная оборудованием и техническими средствами обучения № 3236: *Самарская обл., г. Кинель, п.г.т. Усть-Кинельский, ул. Спортивная, д. 8А.*	Учебная аудитория на 12 посадочных мест, укомплектованная специализированной мебелью (столы, лавки, учебная доска, компьютерные столы, стулья), компьютерной техникой (12 рабочих станций) и техническими средствами обучения (переносной проектор, переносной ноутбук, экран)
2	Помещение для самостоятельной работы, аудитория № 3210 (компьютерный класс) *Самарская обл., г. Кинель, п.г.т. Усть-Кинельский, ул. Спортивная, д. 8А.*	Помещение на 14 посадочных мест, укомплектованное специализированной мебелью (компьютерные столы, стулья) и оснащенное компьютерной техникой (14 рабочих станций), подключенной к сети «Интернет» и обеспечивающей доступ в электронную информационно-образовательную среду университета

8 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1 Виды и формы контроля по дисциплине

Контроль уровня усвоенных знаний, освоенных умений и приобретенных навыков (владений) осуществляется в рамках текущего и промежуточного контроля в соответствии с Положением о текущем контроле и промежуточной аттестации обучающихся.

Текущий контроль освоения компетенций по дисциплине проводится при изучении теоретического материала, выполнении заданий на лабораторных занятиях, выполнении тренингов, устного опроса. Текущему контролю подлежит посещаемость обучающимися аудиторных занятий и работа на занятиях.

Итоговой оценкой освоения компетенций является промежуточная аттестация в форме зачета, проводимая с учетом результатов текущего контроля в 7 семестре на IV курсе очной формы обучения.

8.2 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения образовательной программы в рамках учебной дисциплины

Оценочные средства для проведения текущей аттестации

Тематика тренингов

1. Информационная безопасность сетей.
2. Лицензирование и сертификация в области защиты информации.
3. Уязвимость сети Интернет.
4. Вредоносные программы. Вирусы.
5. Контроль доступа к информации.

Методика проведения тренингов

Тренинг - активный метод социально – психологического обучения, что позволяет за короткий срок не только завладеть большим объемом полезной информации, но и обеспечить формирование и усовершенствование соответствующих профессиональных и практических навыков.

Главная цель тренинга - предоставить максимально приближенные к практическому приложению навыки, которые без дополнительной проработки можно применить в реальной работе.

В тренинге используются проблемные ситуации из реальной деятельности участников, которые проигрываются и анализируются группой при участии специалистов.

Участнику тренинга не надо переводить полученные знания на язык практики, как это обычно происходит в традиционных формах обучения. Знания возникают как результат обобщения и систематизации опыта группы.

В тренинге за счет групповых эффектов достигается комфортная, доброжелательная атмосфера, которая позволяет участникам свободно экспериментировать с новыми способами поведения и применять их на уровне практических умений.

Критерии и шкала оценки при проведении тренингов:

- оценка «зачтено» выставляется обучающимся, если они свободно владеют материалом, ярко и интересно представили свою работу аудитории; сумели ответить на вопросы аудитории; смогли предложить оригинальную идею для решения поставленной задачи.

- оценка «не зачтено» выставляется обучающимся, не владеющим основополагающими знаниями по поставленному вопросу, если они не могут использовать полученные умения и навыки в практической деятельности, путаются в терминологии и не исправляют своих ошибок после наводящих вопросов.

Устный опрос

1. Актуальность информационной безопасности
2. Основные нормативные документы в сфере информационной безопасности
3. Деятельность по обеспечению информационной безопасности.
4. Информационная безопасность сетей.
5. Лицензирование и сертификация в области защиты информации.
6. Уязвимость сети Интернет.
7. Способы совершения компьютерных преступлений.
8. Вредоносные программы. Вирусы.
9. Контроль доступа к информации
10. Принципы, формы и методы деятельности по обеспечению информационной безопасности.
11. Информационная сущность бизнеса.
12. Модель информационной безопасности бизнеса.
13. Модели непрерывного совершенствования и корпоративное управление.
14. Модели непрерывного совершенствования и международные стандарты.
15. Шаги реализации стандартной системы управления информационной безопасностью организации.
16. Формализованное представление угроз информационной безопасности от персонала
17. Противодействие угрозам информационной безопасности от персонала.
18. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса
19. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.
20. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.
21. Подходы к формированию нормативного обеспечения системы информационной безопасности организации
22. Структура документации системы управления информационной безопасностью.
23. Аудит методов и средств обеспечения информационной безопасности организации
24. Аудит интегрированных систем управления.
25. Психологические аспекты подготовки аудитора информационной безопасности.

Критерии и шкала оценки ответов на контрольные вопросы:

- оценка «зачтено» выставляется обучающемуся, если вопросы раскрыты, изложены логично, показано умение иллюстрировать теоретические положения конкретными примерами, продемонстрирована способность использовать сведения из различных источников в реальных условиях; допускаются несущественные ошибки и пробелы в знаниях;

- оценка «не зачтено» выставляется, если уровень знаний обучающегося недостаточен для логичного изложения изучаемого материала, если он неуверенно ориентируется в рекомендуемой литературе, неуверенно или неполно отвечает на дополнительные вопросы.

Оценочные средства для проведения промежуточной аттестации

Зачет проводится по билетам, содержащим 2 теоретических вопроса.

Перечень вопросов к зачету

1. Актуальность информационной безопасности
2. Основные нормативные документы в сфере информационной безопасности
3. Деятельность по обеспечению информационной безопасности.
4. Информационная безопасность сетей.
5. Лицензирование и сертификация в области защиты информации.
6. Уязвимость сети Интернет.
7. Способы совершения компьютерных преступлений.
8. Вредоносные программы. Вирусы.
9. Контроль доступа к информации
10. Принципы, формы и методы деятельности по обеспечению информационной безопасности.
11. Информационная сущность бизнеса.
12. Модель информационной безопасности бизнеса.
13. Модели непрерывного совершенствования и корпоративное управление.
14. Модели непрерывного совершенствования и международные стандарты.
15. Шаги реализации стандартной системы управления информационной безопасностью организации.
16. Формализованное представление угроз информационной безопасности от персонала
17. Противодействие угрозам информационной безопасности от персонала.
18. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса
19. Методы управления информационными рисками. Анализ влияния информационного риска на деятельность организации.
20. Планирование деятельности по обработке рисков обеспечения информационной безопасности организации.
21. Подходы к формированию нормативного обеспечения системы информационной безопасности организации
22. Структура документации системы управления информационной безопасностью.
23. Аудит методов и средств обеспечения информационной безопасности организации
24. Аудит интегрированных систем управления.
25. Психологические аспекты подготовки аудитора информационной безопасности.

Пример билета для зачета

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Самарский государственный аграрный университет»

Специальность: 38.05.01 Экономическая безопасность
Специализация: Экономико-правовое обеспечение экономической безопасности
Кафедра: Менеджмент и маркетинг

Дисциплина «Управление информационными системами
в сфере экономической безопасности»

Билет для зачета № 1

1. Информационная сущность бизнеса.
2. Способы совершения компьютерных преступлений.

Составитель _____ И.Н. Мамай

Заведующий кафедрой _____ А.Г. Волконская
«___» _____ 20__ г.

Пример эталонного ответа на вопросы билета

1.Информационная сущность бизнеса. Информация является неотъемлемой частью бизнеса. Бизнес-процессы не могут существовать без информации и вне информации, хотя бы потому, что бизнес существует в рамках определенной правовой среды, определяемой совокупностью информационных объектов, таких как законодательные и нормативные акты, постановления правительства и других подобных документов, и формирует отчетность по нормам этой правовой среды, т. е. порождает информацию определенного вида. Сущность бизнес процесса представляется как процесс достижения некоторой совокупности целей (бизнес-целей) на основе управления активами. Информационной сущностью бизнеса и является этот процесс управления. Если правовое поле, отчетность, активы и возможные операции над ними во многом зависят от природы бизнеса, то процесс управления в большой степени инвариантен к ней.

Главная особенность управления в бизнесе, существенно отличающая его от некоторых других, например, технических систем автоматического управления и регулирования, является большая задержка между моментом принятия решения и получаемым результатом.

После принятия решений по управлению реализуется некий процесс бизнеса, протекающий в слабо детерминированной внешней среде, не все параметры которой контролируются организацией, осуществляющей бизнес. Таким образом, результат принятых решений наблюдается с задержкой и иногда весьма значительной. Поэтому важнейшей для бизнеса является способность предвидеть возникновение разного рода ситуаций (как благоприятных, так и неблагоприятных) в среде бизнеса и в самом бизнесе. Это чисто информационная задача, в основе которой лежит прогноз.

Когда задумывается и реализуется какой-либо процесс целенаправленной деятельности необходимо поставить и ответить на следующие вопросы:

- будет ли достигнута цель в том виде, как предполагается?
- достаточно ли в нашем распоряжении операционных возможностей, знаний (опыта), соответствует ли потребностям качество подготовки персонала и система менеджмента?
- достаточно ли привлечено ресурсов для достижения поставленной цели?

- достаточен ли интервал времени, устанавливаемый для достижения цели?

Из поставленных вопросов видно, что ответы на них требуют анализа различных информационных сущностей, описывающих в формализованном или неформализованном виде различные аспекты деятельности, отраженные в заданных вопросах. Ясно, что ответы на эти вопросы могут быть получены только в виде прогнозов, т. е. тоже в виде информационных сущностей. Очевидно также, что все вопросы взаимозависимы и, следовательно, ответы на них должны быть взаимоувязаны. Совокупная погрешность ответов на вопросы создает консолидированный риск достижения цели. Величина этого риска зависит еще и от того, насколько изменятся условия реализации цели в процессе ее достижения, и от характера этих изменений.

2. Способы совершения компьютерных преступлений. Одним из основных элементов криминалистической характеристики преступлений в сфере компьютерной информации являются способы совершения преступлений, которые группируются следующим образом: методы перехвата компьютерной информации; методы несанкционированного доступа; метод манипуляции; комплексные методы.

Методы перехвата компьютерной информации.

- Непосредственный (активный) перехват. Осуществляется путем непосредственного подключения к телекоммуникационному оборудованию компьютера или компьютерной сети. Перехват и запись данных происходит через телефонный канал системы, либо подключением к линии принтера;
- Электромагнитный (пассивный) перехват. Основан на способности дипольной антенны, подключенной к телевизору и видеомагнитофону, улавливать излучение процессора и монитора компьютера и считывать с них компьютерную информацию с расстояния до 1000 метров;
- Аудиоперехват. Выделяются два его варианта: заходовый (путем установки прослушивающих устройств — «жучков» в охраняемом помещении) и беззаходовый (путем установки акустических и вибрационных датчиков съема информации — дистанционно- направленных микрофонов, находящихся за пределами охраняемого помещения) с целью прослушивания разговоров работающего на ЭВМ персонала и звуковых сигналов технических устройств (телефонов, принтеров);
- Видеоперехват («откачивание данных»). Направлен на получение компьютерной информации с монитора или нажимаемых клавиатурных клавиш с помощью различных оптических приборов (биноклей, подзорных труб, видеокамер и т.п.);
- «Уборка мусора». Состоит в поиске технологических отходов, оставленных пользователем после работы с компьютером. Включает как физический вариант (осмотр содержимого мусорных корзин и сбор оставленных за ненадобностью распечаток, деловой переписки и т.п.), так и электронный вариант, основанный на том, что последние из сохраненных данных обычно не стираются после завершения работы. Другой пользователь записывает только небольшую часть своей информации, а затем спокойно считывает предыдущие записи, выбирая нужную ему информацию.

Получив необходимый объем предварительной компьютерной информации, преступник затем осуществляет несанкционированное вторжение в ЭВМ. Для этого ему необходимо знать номер телефона или иметь доступ к телефонной линии связи, иметь код пользователя и пароль.

Методы несанкционированного доступа. Существуют следующие основные методы несанкционированного доступа к компьютерной информации:

1. «За дураком». Используется для входа в закрытые для доступа помещения или терминалы. Выделяются два его варианта: физический вариант (взяв в руки как можно больше предметов, связанных с работой на компьютере, попытаться уверенно пройти в дверь терминала вслед за законным пользователем) и электронный вариант (компьютер незаконного поль-

зователя подключается к линии законного через телефонные каналы (Интернет) или в тот момент, когда пользователь выходит ненадолго из терминала, оставляя компьютер в активном режиме).

2. «За хвост». Незаконный пользователь подключается к линии связи законного пользователя, а затем, дождавшись сигнала, обозначающего конец работы, перехватывает его и входит в систему в тот момент, когда законный пользователь заканчивает активный режим.

3. Компьютерный «абордаж». Осуществляется путем случайного подбора абонентского телефонного номера модема, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственной ЭВМ, и связь установлена. Затем производится подбор кода (пароля) доступа к чужому компьютеру, что позволяет внедриться в чужую компьютерную систему.

4. «Неспешный выбор». Несанкционированный доступ к файлам законного пользователя осуществляется нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может не спеша исследовать компьютерную информацию и многократно копировать ее.

5. «Брешь». Данный метод аналогичен предыдущему, но основан на ошибках или неудачной логике построения компьютерных программ.

6. «Системные ротозеи». Несанкционированный доступ осуществляется нахождением «бреши» в программе входа в систему.

7. «Люк» («задние ворота») — это не описанные в документации возможности работы с компьютерными программами. В найденной «бреши» программа «разрывается» и туда дополнительно вставляют одну или несколько команд. Этот «люк» «открывается» по мере необходимости и встроенные команды автоматически начинают выполнять свою задачу. Создание и использование «люка» образует состав преступления, предусмотренный ст. 273 УК РФ.

8. «Маскарад» («самозванство», «узурпация личности»). Заключается в проникновении в компьютерную систему путем выдачи себя за законного пользователя. Самый простейший путь его осуществления — получить коды (пароли) законных пользователей.

9. Мистификация. Пользователь с удаленного терминала случайно подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеревался. Владелец этой системы, формируя правдоподобные отклики, может какое-то время поддерживать это заблуждение, получая информацию.

10. «Аварийный». Используется тот факт, что в любом компьютерном центре имеется особая программа, применяемая в случае возникновения сбоев или других отклонений в работе ЭВМ. Осуществляется путем незаконного использования универсальных программ («Супервизор»), применяемых в аварийных ситуациях, с помощью которых возможен доступ к компьютеру, минуя все средства защиты и контроля.

11. «Склад без стен». Несанкционированный доступ осуществляется в результате использования системной поломки, в результате которой возникает нарушение нормального функционирования систем зашиты данных.

12. «Подкладывание свиньи». Осуществляется путем подключения к линиям связи и имитации работы системы с целью получения незаконных манипуляций.

Методы манипуляции с компьютерной информацией. К ним относятся следующие:

- Подмена данных — изменение или введение новых данных осуществляется, как правило, при вводе или выводе информации с ЭВМ. Выделяются два его варианта: манипуляции по входу и манипуляции по выходу.
- Подмена кода. Заключается в изменении кода данных, например бухгалтерского учета.
- «Асинхронная атака». Основывается на совмещении команд двух и более пользователей, чьи программы ЭВМ выполняет одновременно (параллельно) и одной из которых является программа преступника.
- «Пинание». Преступник выводит из строя электронный адрес, бомбардируя его многочисленными почтовыми сообщениями.

Комплексные методы. Как правило, компьютерные преступления совершаются с помощью того или иного сочетания приемов. Существуют следующие основные комплексные методы манипуляций с компьютерной информацией:

1. «Воздушный змей». Суть метода заключается в том, чтобы замаскировать путем многократных переводов денежных средств из одного банка в другой необеспеченный денежными средствами перевод.

2. «Ловушка на живца». Заключается в создании преступником специальной программы, которая записывается на физический носитель и передается потерпевшей стороне. При работе этой программы автоматически моделируется системная поломка компьютера, а затем, при проверке компьютера на работоспособность, программа записывает интересующую преступника информацию. В последующем программа изымается у потерпевшей стороны под благовидным предлогом.

3. «Раздеватели» — это комплекс специальных программ, ориентированных на исследования защитного механизма программ от несанкционированного копирования и его преодоление.

4. «Троянский конь». Осуществляется путем тайного ввода в чужую программу команд, позволяющих, не изменяя работоспособность программы, осуществить определенные функции. Этим способом преступники обычно отчисляют на свой банковский счет определенную сумму с каждой операции в банке.

8.3 Критерии оценивания уровня сформированности компетенций

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов знать, уметь, владеть заявленных дисциплинарных компетенций проводится по 2-х бальной шкале оценивания путем выборочного контроля во время зачета.

Шкала оценивания зачета

Результат зачета	Критерии
«зачтено»	Ответ обучающегося на вопрос должен быть полным и развернутым, ни в коем случае не зачитываться дословно, содержать четкие формулировки всех определений, касающихся указанного вопроса, подтверждаться фактическими примерами. Такой ответ должен продемонстрировать знание обучающимся материала лекций, базовой и дополнительной литературы
«не зачтено»	Ответ обучающегося на вопрос содержит неправильные формулировки основных определений, прямо относящихся к вопросу, или обучающийся вообще не может их дать, как и подтвердить свой ответ фактическими примерами. Такой ответ демонстрирует незнание материала дисциплины

8.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций по дисциплине «Управление информационными системами в сфере экономической безопасности» проводится в форме текущей и промежуточной аттестации.

Контроль текущей успеваемости обучающихся – текущая аттестация – проводится в ходе семестра с целью определения уровня усвоения обучающимися знаний; формирования у них умений и навыков; своевременного выявления преподавателем недостатков в подготовке обучающихся и принятия необходимых мер по ее корректировке; совершенствованию методики обучения; организации учебной работы и оказания обучающимся индивидуальной помощи.

К контролю текущей успеваемости относятся проверка знаний, умений и навыков обучающихся:

▪ на занятиях (тренинги, опросы);

▪ по результатам проверки качества конспектов лекций и иных материалов;

▪ по результатам отчета обучающихся в ходе индивидуальной консультации преподавателя, проводимой в часы самоподготовки, по имеющимся задолженностям.

Контроль за выполнением обучающимися каждого вида работ может осуществляться поэтапно и служит основанием для предварительной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится с целью выявления соответствия уровня теоретических знаний, практических умений и навыков по дисциплине требованиям ФГОС по специальности в форме зачета.

Зачет проводится после завершения изучения дисциплины в объеме рабочей учебной программы. Форма проведения зачета – устно. Оценка по результатам зачета – «зачтено» и «не зачтено».

Все виды текущего контроля осуществляются на практических занятиях.

Каждая форма контроля по дисциплине включает в себя теоретические вопросы, позволяющие оценить уровень освоения обучающимися знаний и практические задания, выявляющие степень сформированности умений и навыков.

Процедура оценивания компетенций, обучающихся основана на следующих стандартах:

1. Периодичность проведения оценки (на каждом занятии).

2. Многоступенчатость: оценка (как преподавателем, так и обучающимися группы) и самооценка обучающегося, обсуждение результатов и комплекса мер по устранению недостатков.

3. Единство используемой технологии для всех обучающихся, выполнение условий сопоставимости результатов оценивания.

4. Соблюдение последовательности проведения оценки: предусмотрено, что развитие компетенций идет по возрастанию их уровней сложности, а оценочные средства на каждом этапе учитывают это возрастание.

Краткая характеристика процедуры реализации текущего контроля и промежуточной аттестации по дисциплине для оценки компетенций обучающихся представлена в таблице:

№ п/п	Наименование оценочного средства	Краткая характеристика процедуры оценивания компетенций	Представление оценочного средства в фонде
1	Тренинг	Активный метод социально – психологического обучения, который позволяет за короткий срок не только завладеть большим объемом полезной информации, но и обеспечить формирование и усовершенствование соответствующих профессиональных и практических навыков. Позволяет оценить владение новыми способами поведения на уровне практических умений.	Тематика тренингов
2	Устный опрос	Устный опрос по контрольным вопросам может проводиться в начале/конце практического занятия, либо в течение всего практического занятия по заранее выданной тематике. Выбранный преподавателем обучающийся может отвечать с места либо у доски.	Контрольные вопросы по темам дисциплины
3	Зачет	Проводится в заданный срок, согласно графику учебного процесса. При	Комплект вопросов к зачету

		выставлении оценок учитывается уровень приобретенных компетенций обучающегося. Компонент «знать» оценивается теоретическими вопросами по содержанию дисциплины, компоненты «уметь» и «владеть» - практико-ориентированными заданиями	

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования (ФГОС ВО).

Рабочую программу разработал:
доцент кафедры «Менеджмент и маркетинг»,
канд. пед. наук, доцент И.Н. Мамай _____

Рассмотрена и одобрена на заседании кафедры «Менеджмент и маркетинг» 5 апреля 2022 г., протокол № 8.

Заведующий кафедрой
канд. экон. наук, доцент А.Г. Волконская _____

СОГЛАСОВАНО:

Председатель методической комиссии
экономического факультета
канд. экон. наук Н.Н. Липатова _____

Руководитель ОПОП ВО
канд. экон. наук, доцент Ю.Ю. Газизьянова _____

Начальник УМУ
канд. техн. наук, доцент С.В. Краснов _____

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ В РАБОЧЕЙ ПРОГРАММЕ
на 2023 /2024 учебный год

В рабочую программу дисциплины «Управление информационными системами в сфере экономической безопасности» вносятся следующие изменения:

1. Согласно СМК 04-06-2023 «Положение о порядке разработки и утверждения рабочей программы дисциплины (модуля)» таблицу в разделе 3 рабочей программы представить в следующем виде:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения по дисциплине
ПК-3 Способен реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать и использовать в интересах выявления рисков, локализации и нейтрализации угроз экономической безопасности, пресечения и расследования преступлений и иных правонарушений в сфере экономики	ИД-1/ПК-3 Знает законодательство, нормативные правовые акты и правила внутреннего распорядка в целях экономической безопасности, перечень и признаки экономических преступлений в отношении хозяйствующего субъекта	Знать: правовые основы в области экономической безопасности, перечень и признаки экономических преступлений в отношении хозяйствующего субъекта Умеет проводить анализ признаков экономических преступлений в отношении хозяйствующего субъекта Владеет: навыками работы с законодательством, нормативными правовыми актами и правилами внутреннего распорядка, анализа признаков экономических преступлений в отношении хозяйствующего субъекта
	ИД-2/ПК-3 Определяет источники информации для проведения финансового расследования в целях экономической безопасности организации	Знает: источники и формы отчетности, используемые для исследования финансовых процессов и прогнозирования угроз экономической безопасности Умеет: использовать источники и формы отчетности, используемые для исследования финансовых процессов и прогнозирования угроз экономической безопасности Владеет: навыками выбора источников и форм отчетности, используемых для исследования финансовых процессов и прогнозирования угроз экономической безопасности
	ИД-3/ПК-3 Подготавливает аналитические материалы о выявлении в организации операций (сделок), имеющих признаки неправомерности и необычности	Знает: фирмы и способы подготовки аналитических материалы о выявлении в организации операций (сделок), имеющих признаки неправомерности и необычности Умеет: подготовить аналитические материалы о выявлении в организации операций (сделок), имеющих признаки неправомерности и необычности Владеет: навыками подготовки аналитических материалов о выявлении в организации операций (сделок), имеющих признаки неправомерности и необычности
	ИД-4/ПК-3 Выполняет экспертные процедуры с использованием современных подходов и методов, информационных технологий и программных продуктов	Знает: современные подходы и методы, информационные технологии и программные продукты Умеет: выполнять экспертные процедуры и применять современные подходы и методы, информационные технологии и программные продукты Владеет: навыками экспертных процедур и применения современных подходов и методов, информационных технологий и программных продуктов

2. Раздел 6 рабочей программы представить в следующей редакции:

6.1. Основная литература:

6.1.1. Столетова, Е. А. Информационные системы и технологии в экономике и управлении : учебное пособие / Е. А. Столетова, Л. А. Яковлева. — Кемерово : КемГУ, 2018. — 173 с. – URL: https://e.lanbook.com/book/107711

6.1.2. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. – URL: https://e.lanbook.com/book/130184

6.2. Дополнительная литература:

6.2.1. Бочков, А. П. Информационные системы управления экономическими объектами : учебник / А. П. Бочков, А. А. Графов. — 2-е изд., перераб. и доп. — Санкт-Петербург : Лань, 2022. — 160 с. – URL: https://e.lanbook.com/book/206870

6.2.2. Дешко, И. П. Управление сетевыми информационными системами: Курс лекций : учебное пособие / И. П. Дешко, К. Г. Кряженков. — Москва : РТУ МИРЭА, 2021. — 174 с. – URL: https://e.lanbook.com/book/176536

6.2.3. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. – URL: https://e.lanbook.com/book/207095

Шашкова, И. Г. Информационные системы и технологии / В. С. Конкина, Е. И. Машкова; И. Г. Шашкова. – : [Б.и.], 2013. – 541 с. – Режим доступа: https://rucont.ru/efd/225944

6.3. Программное обеспечение:

6.3.1. MicrosoftWindows 7 Профессиональная 6.1.7601ServicePack 1;

6.3.2. Microsoft Windows SL 8.1 RU AE OLP NL;

6.3.3. Microsoft Office Standard 2010;

6.3.4. Microsoft Office стандартный 2013;

6.3.5. Kaspersky Endpoint Security для бизнеса - стандартный Russian Edition;

6.3.6. WinRAR:3.x: Standard License – educational –EXT;

6.3.7. 7 zip (свободный доступ).

6.4. Перечень информационно-справочных систем и профессиональных баз данных:

6.4.1. http://www.consultant.ru – Справочная правовая система «Консультант Плюс».

6.4.2. http://www.garant.ru – Справочно-правовая система по законодательству Российской Федерации «Гарант».

6.4.3. www.elibrary.ru – Научная электронная библиотека.

3. С 01.09.2023 года дисциплина закреплена за кафедрой «Государственное управление и деловое администрирование» в связи с решением ученого совета Университета (протокол №8 от 27.04.2023 г.) в целях оптимизации структурных подразделений экономического факультета.

Дополнения и изменения в рабочей программе рассмотрены и одобрены на заседании кафедры «Менеджмент и маркетинг» 2 мая 2023 г., протокол № 9.

Дополнения и изменения согласованы с методической комиссией факультета.

Председатель методической комиссии
экономического факультета,
канд.экон.наук., доцент  Ю.Н. Кудряшова