УТВЕРЖДАЮ:
Директор Института
экономики и управления АПК
_____ Л.И. Хоружий
«30» «апреля» 2022 г.

Лист актуализации рабочей программы дисциплины
Б1.В.11 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И БЕЗОПАСНОСТЬ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

для подготовки магистров
Направление: 42.04.01 Реклама и связи с общественностью
Направленность: «Реклама и связи с общественностью в отрасли (в сфере АПК)»
Форма обучения – очная
Год начала подготовки: 2019

Курс 2
Семестр 3

В рабочую программу вносятся изменения:
1. По формулировке направленности «Стратегические коммуникации в условиях цифровизации».
2. По формулировке компетенций

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикатор компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
1.	**ПКос-3**	Способен применять в профессиональной деятельности комплекс современных технолог	**ПКос-3.1** Использует современные технологии формирования взаимоотношений и встраивания онлайн и	Современные технологии формирования взаимоотношений и встраивания онлайн и офлайн коммуникаций с различными стейкхолдерам	Применять современные технологии формирования взаимоотношений и встраивания онлайн и офлайн коммуникаций с различными	Современными технологиями формирования взаимоотношений и встраивания онлайн и офлайн коммуникаций с различными стейкхолдерами с учетом информационной

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикатор компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
		ических решений, технических средств, приемов и методов онлайн и офлайн коммуникаций в условиях цифровизации	офлайн коммуникаций с различными стейкхолдерами	и с учетом информационной безопасности	стейкхолдерами с учетом информационной безопасности	безопасности
2.	**ПКос-1**	Способен к руководству подразделением (компании) в сфере рекламы и связей с общественностью, организации и управлению коммуникационными проектами и мероприятиями	**ПКос-1.1** Выполняет функционал руководителя линейного/функционального подразделения отдела по рекламе и (или) связям с общественностью организации или коммуникационного/рекламного/ PR-агентства в условиях цифровизации	Функционал руководителя линейного/функционального подразделения отдела по рекламе и (или) связям с общественностью организации или коммуникационного/рекламного/ PR-агентства с учетом информационной безопасности	Применять функционал руководителя линейного/функционального подразделения отдела по рекламе и (или) связям с общественностью организации или коммуникационного/рекламного/ PR-агентства с учетом информационной безопасности	Навыками руководства компании в сфере рекламы и связей с общественностью, организации и управления коммуникационными проектами и мероприятиями с учетом информационной безопасности
			ПКос-1.2 Осуществляе	Функции организации и	Применять функции	Навыками в организации и

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикатор компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
			т функции организации и управления коммуникационными проектами и мероприятиями, контролирует и оценивает их эффективность	управления коммуникационными проектами и мероприятиями, методы контроля и оценки их эффективности. Методы и средства по обеспечению информационной безопасности в профессиональной деятельности	организации и управления коммуникационными проектами и мероприятиями, методы контроля и оценки их эффективности. Использовать методы и средства по обеспечению информационной безопасности в профессиональной деятельности	управлении коммуникационными проектами и мероприятиями, контролируя и оценивая их эффективность с учетом информационной безопасности

Программа актуализирована для Учебного плана 2022 года начала подготовки, направленности «Стратегические коммуникации в условиях цифровизации».

Разработчики: Лемешко Т.Б., ст. преподаватель _____

Худякова Е.В., д.э.н., профессор _____

Рабочая программа пересмотрена и одобрена на заседании кафедры прикладной информатики, протокол № 1 от «29» августа 2022 г.

Заведующий кафедрой _____Е.В. Худякова

Лист актуализации принят на хранение:

И.о. заведующего выпускающей кафедрой связей с общественностью, речевой коммуникации и туризма Гнездилова Е.В., к.ф.н., доцент

_____ «30» августа 2022 г.

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ – МСХА имени К.А. ТИМИРЯЗЕВА»
(ФГБОУ ВО РГАУ - МСХА имени К.А. Тимирязева)

Институт экономики и управления АПК
Кафедра прикладной информатики

УТВЕРЖДАЮ:
И.о. декана гуманитарно-педагогического факультета
_____ П.Ф. Кубрушко
_____2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.11 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И БЕЗОПАСНОСТЬ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

для подготовки магистров

ФГОС ВО

Направление: 42.04.01 Реклама и связи с общественностью
Направленность: «Реклама и связи с общественностью в отрасли (в сфере АПК)»

Курс 2
Семестр 3

Форма обучения: очная

Год начала подготовки: 2019

Регистрационный номер _____

Москва, 2020

Разработчик: Худякова Е.В., д.э.н., профессор _____
Лемешко Т.Б., старший преподаватель _____
«13» 01 2020 г.

Рецензент: Остапчук Т.В., к.э.н., доцент _____
(подпись)
«13» 01 2020 г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 42.04.01 Реклама и связи с общественностью и учебного плана по данному направлению 2019 года начала подготовки.

Программа обсуждена на заседании кафедры прикладной информатики протокол № 5 от «14» 01 2020 г.

Зав. кафедрой: Худякова Е.В., д.э.н., профессор _____
(ФИО, ученая степень, ученое звание) (подпись)
«14» 01 2020 г.

Согласовано:
Председатель учебно-методической
комиссии гуманитарно-педагогического факультета,
Ерёмин В.И., д.э.н., профессор _____
(ФИО, ученая степень, ученое звание) (подпись)
Протокол №7 «10» 02 2020 г.

Заведующий выпускающей кафедрой связей с общественностью и речевой коммуникации,
Бугаёва И.В., д.ф.н., профессор _____
(ФИО, ученая степень, ученое звание) (подпись)
«10» 02 2020 г.

Заведующий отделом комплектования ЦНБ _____ / Иванова Л.И.
(подпись)

Бумажный экземпляр РПД, копии электронных вариантов РПД и оценочных материалов получены:
Методический отдел УМУ

_____ «__» _____2020 г.

СОДЕРЖАНИЕ

АННОТАЦИЯ
рабочей программы учебной дисциплины
Б1.В.11 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И БЕЗОПАСНОСТЬ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»,
для подготовки магистра по направлению
42.04.01 Реклама и связи с общественностью,
направленности «Реклама и связи с общественностью в отрасли (в сфере АПК)»

Цель освоения дисциплины: повышение уровня грамотности, информационной культуры в сфере информационной безопасности, формирование культуры личной информационной безопасности; обучение магистров принципам, методам и средствам по обеспечению информационной безопасности в профессиональной деятельности, при формировании взаимоотношений и встраивании онлайн и офлайн коммуникаций с различными стейкхолдерами, при организации и управлении коммуникационными проектами и мероприятиями, при выполнении функционала руководителя линейного/функционального подразделения отдела по рекламе и связям с общественностью.

Место дисциплины в учебном плане: дисциплина включена в часть, формируемая участниками образовательных отношений учебного плана по направлению подготовки 42.04.01 Реклама и связи с общественностью.

Требования к результатам освоения дисциплины: в результате освоения дисциплины формируются следующие компетенции (индикаторы): **ПКос-3.1; ПКос-1.1; ПКос-1.2**

Краткое содержание дисциплины:

Основы информационной безопасности и защиты информации. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности. Административный и процедурный уровни обеспечения информационной безопасности. Основные программно-технические меры обеспечения информационной безопасности. Информационная безопасность в профессиональной деятельности.

Общая трудоемкость дисциплины: 72/2 (часы/зач. ед.).

Промежуточный контроль: зачёт в 3 семестре.

1. Цель освоения дисциплины

Целью освоения дисциплины «Информационная безопасность и безопасность профессиональной деятельности» является повышение уровня грамотности, информационной культуры в сфере информационной безопасности, формирование культуры личной информационной безопасности; обучение магистров принципам, методам и средствам по обеспечению информационной безопасности в профессиональной деятельности, при формировании взаимоотношений и встраивании онлайн и офлайн коммуникаций с различными стейкхолдерами, при организации и управлении коммуникационными проектами и мероприятиями, при выполнении

функционала руководителя линейного/функционального подразделения отдела по рекламе и связям с общественностью.

2. Место дисциплины в учебном процессе

Дисциплина «Информационная безопасность и безопасность профессиональной деятельности» включена в часть, формируемая участниками образовательных отношений учебного плана по направлению подготовки 42.04.01 Реклама и связи с общественностью. Дисциплина «Информационная безопасность и безопасность профессиональной деятельности» реализуется в соответствии с требованиями ФГОС ВО, ОПОП ВО и Учебного плана по направлению подготовки 42.04.01 Реклама и связи с общественностью.

Предшествующими курсами, на которых непосредственно базируется дисциплина «Информационная безопасность и безопасность профессиональной деятельности» являются: «Цифровые коммуникации и новые медиа», «Управление отделом рекламы, связей с общественностью и пресс-службой»

Дисциплина «Информационная безопасность и безопасность профессиональной деятельности» является основополагающей для изучения следующих дисциплин: «Документоведение и тендерная документация», «Стратегические коммуникации в сфере АПК», «Планирование и реализация кампаний по рекламе и связям с общественностью».

Рабочая программа дисциплины «Информационная безопасность и безопасность профессиональной деятельности» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития индивидуальных возможностей и состояния здоровья таких обучающихся.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций, представленных в таблице 1.

Таблица 1

Требования к результатам освоения учебной дисциплины

№ п/п	Код компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	В результате изучения учебной дисциплины обучающиеся должны:		
				знать	уметь	владеть
1.	**ПКос-3**	Способен применять в профессиональной деятельности комплекс современных технологических решений, технических средств, приемов и методов онлайн и офлайн коммуникаций	**ПКос-3.1** Использует современные технологии формирования взаимоотношений и встраивания онлайн и офлайн коммуникаций с различными стейкхолдерами	Современные технологии формирования взаимоотношений и встраивания онлайн и офлайн коммуникаций с различными стейкхолдерами с учетом информационной безопасности	Применять современные технологии формирования взаимоотношений и встраивания онлайн и офлайн коммуникаций с различными стейкхолдерами с учетом информационной безопасности	Современными технологиями формирования взаимоотношений и встраивания онлайн и офлайн коммуникаций с различными стейкхолдерами с учетом информационной безопасности
2.	**ПКос-1**	Способен к руководству подразделением (компании) в сфере рекламы и связей с общественностью, организации и управлению коммуникационными проектами и мероприятиями	**ПКос-1.1** Выполняет функционал руководителя линейного/функционального подразделения отдела по рекламе и (или) связям с общественностью организации или коммуникационного/рекламного/ PR-агентства	Функционал руководителя линейного/функционального подразделения отдела по рекламе и (или) связям с общественностью организации или коммуникационного/рекламного/ PR-агентства с учетом информационной безопасности	Применять функционал руководителя линейного/функционального подразделения отдела по рекламе и (или) связям с общественностью организации или коммуникационного/рекламного/ PR-агентства с учетом информационной безопасности	Навыками руководства компании в сфере рекламы и связей с общественностью, организации и управления коммуникационными проектами и мероприятиями с учетом информационной безопасности
			ПКос-1.2 Осуществляет функции организации и управления коммуникационными проектами и мероприятиями, контролирует и оценивает их эффективность	Функции организации и управления коммуникационными проектами и мероприятиями, методы контроля и оценки их эффективности. Методы и средства по обеспечению информационной безопасности в профессиональной деятельности	Применять функции организации и управления коммуникационными проектами и мероприятиями, методы контроля и оценки их эффективности. Использовать методы и средства по обеспечению информационной безопасности в профессиональной деятельности	Навыками в организации и управлении коммуникационными проектами и мероприятиями, контролируя и оценивая их эффективность с учетом информационной безопасности

4. Структура и содержание дисциплины

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 2 зач. единицы (72 часа), их распределение по видам работ в 3 семестре представлено в таблице 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость	
	час.	в т.ч. по семестрам
		№ 3
Общая трудоёмкость дисциплины по учебному плану	**72**	**72**
1. Контактная работа:	**16,25**	**16,25**
Аудиторная работа	**16,25**	**16,25**
лекции (Л)	4	4
практические занятия (ПЗ)	12	12
контактная работа на промежуточном контроле (КРА)	0,25	0,25
2. Самостоятельная работа (СРС)	**55,75**	**55,75**
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к практическим занятиям и т.д.)	46,75	46,75
Подготовка к зачёту (контроль)	9	9
Вид промежуточного контроля:		Зачёт

4.2 Содержание дисциплины

Таблица 3

Тематический план учебной дисциплины

Наименование тем дисциплины	Всего часов	Аудиторная Работа			Внеаудиторная работа (СРС)
		Л	ПЗ	ПКР	
Тема 1. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	20	-	2	-	18
Тема 2. Программно-технические меры обеспечения информационной безопасности	20	2	4	-	14
Тема 3. Информационная безопасность в профессиональной деятельности	31,75	2	6	-	23,75
Контактная работа на промежуточном контроле (КРА)	0,25	-	-	0,25	-
ИТОГО	**72**	**4**	**12**	**0,25**	**55,75**

Тема 1. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности

Актуальность проблемы обеспечения безопасности в цифровом обществе. Основные понятия и определения информационной безопасности. Основные составляющие информационной безопасности. Наиболее распространенные

угрозы информационной безопасности. Виды мер обеспечения информационной безопасности.

Обзор российского законодательства в области информационной безопасности. Стандарты и спецификации в области информационной безопасности. Морально-этические нормы поведения в цифровом мире. Организационно-правовые механизмы обеспечения информационной безопасности предприятия. Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 5.12.2016 г. Закон 149-ФЗ «Об информации…». Закон 1-ФЗ «Об электронной цифровой подписи». Закон 63-ФЗ «Об электронной подписи». Обзор зарубежного законодательства в области информационной безопасности. Сетевые сервисы безопасности по уровням модели OSI. Сетевые механизмы безопасности. Администрирование средств безопасности. Критерии оценки информационной безопасности ISO/IEC 15408. Российское и международное законодательство в области защиты прав на интеллектуальную собственность. Административный и процедурный уровни обеспечения информационной безопасности. Анализ рисков информационной безопасности. Политика информационной безопасности. Программа работ в области обеспечения информационной безопасности. Основные классы мер процедурного уровня: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ.

Тема 2. Программно-технические меры обеспечения информационной безопасности

Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Технологии защиты данных. Идентификация и аутентификация, управление доступом. Шифрование, контроль целостности. Криптографические алгоритмы. Анализ защищенности. Обеспечение высокой доступности. Сервисы безопасности. Классификация сервисов безопасности с точки зрения места в общей архитектуре мер

безопасности. Технологии защиты межсетевого обмена данными. Методы управления средствами сетевой безопасности.

Тема 3. Информационная безопасность в профессиональной деятельности

Организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия. Основные риски и угрозы информационной безопасности компании в сфере рекламы и связей с общественностью. Безопасное использование интернета в подразделениях компании в сфере рекламы и связей с общественностью. Антивирусная защита информационных ресурсов компании по рекламе и СО. Контентная фильтрация. Защита персональных данных. Создание системы защиты информации в организации: этапы создания системы защиты информации, классификация организационно-технологических мероприятий по защите информации, общие требования к системе защиты информации. Методы защиты онлайн и офлайн коммуникации.

4.3 Лекции/практические занятия

Таблица 4

Содержание лекций/ практических занятий и контрольные мероприятия

№ п/п	№ темы	№ и название лекций/ практических занятий	Форми-руемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов
1.	Тема 1. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности	Практическое занятие № 1. Анализ стандартов. Поиск и анализ законодательных актов по ИБ в справочно-правовой системе КонсультантПлюс. Анализ рисков ИБ.	ПКос-3.1; ПКос-1.1; ПКос-1.2	защита практической работы № 1, устный опрос № 1	2
2.	Тема 2. Программно-технические меры обеспечения информационной безопасности	Лекция № 1. Технологии защиты информации. Криптография. Электронная цифровая подпись.	ПКос-3.1; ПКос-1.1; ПКос-1.2	-	2
		Практическое занятие № 2. Шифрование. Идентификация и аутентификация.	ПКос-3.1; ПКос-1.1; ПКос-1.2	защита практической работы № 2, устный опрос № 2	4

№ п/п	№ темы	№ и название лекций/ практических занятий	Форми-руемые компетенции (индикаторы)	Вид контрольного мероприятия	Кол-во часов
3.	Тема 3. Информационная безопасность в профессиональной деятельности	Лекция № 2. Информационная безопасность компании по рекламе и связям с общественностью	ПКос-3.1; ПКос-1.1; ПКос-1.2	-	2
		Практическое занятие № 3. Методы защиты онлайн и офлайн коммуникации. Сетевые сервисы Web 2.0: создание ментальных карт и др.	ПКос-3.1; ПКос-1.1; ПКос-1.2	защита практической работы № 3	6

Таблица 5

Перечень вопросов для самостоятельного изучения дисциплины

№ п/п	№ темы	Перечень рассматриваемых вопросов для самостоятельного изучения
1.	Тема 1. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности.	1. Актуальность проблемы обеспечения безопасности в цифровом обществе, в условиях цифровой экономики и цифровых коммуникаций. 2. Законодательные акты РФ, регулирующие правовые отношения в сфере информационной безопасности и защиты государственной тайны. 3. Морально-этические нормы поведения в цифровом мире. ПКос-3.1; ПКос-1.1; ПКос-1.2
2.	Тема 2. Программно-технические меры обеспечения информационной безопасности	1. Методы управления средствами сетевой безопасности. 2. Технологии обнаружения вторжений. 3. Инфраструктура защиты на прикладном уровне. 4. Технологии межсетевых экранов. 5. Обеспечение безопасности операционных систем. 6. Технологии аутентификации ПКос-3.1; ПКос-1.1; ПКос-1.2
3.	Тема 3. Информационная безопасность в профессиональной деятельности	1. Основные риски и угрозы информационной безопасности компании в сфере рекламы и связей с общественностью. 2. Создание системы защиты информации в организации: этапы создания системы защиты информации, классификация организационно-технологических мероприятий по защите информации, общие требования к системе защиты информации. 3. Способы защиты цифровых коммуникаций. ПКос-3.1; ПКос-1.1; ПКос-1.2

5. Образовательные технологии

Таблица 6

Применение активных и интерактивных образовательных технологий

№ п/п	Раздел и форма занятия		Наименование используемых активных и интерактивных образовательных технологий
1.	Технологии защиты информации. Криптография. Электронная цифровая подпись.	Л	Интерактивная лекция
2.	Шифрование. Идентификация и аутентификация.	ПЗ	Групповое обсуждение
3.	Методы защиты онлайн и офлайн коммуникации. Сетевые сервисы Web 2.0: создание ментальных карт и др.	ПЗ	Групповое обсуждение
4	Информационная безопасность компании по рекламе и связям с общественностью	Л	Интерактивная лекция

6. Текущий контроль успеваемости и промежуточная аттестация по итогам освоения дисциплины

6.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

1) Примеры заданий практических работ

Пример задания по теме 1 : «Законодательный и нормативно-правовой уровни обеспечения информационной безопасности»

Используя информационную систему Консультант Плюс, найти и отобразить с добавлением в раздел «Избранное» и экспортом в Microsoft Word:

1) основные нормативно-правовые акты, регулирующие деятельность в информационной сфере.

2) определения основных категорий информационной безопасности.

3) подборку статей по защите информации.

Примеры заданий по теме 2. «Программно-технические меры обеспечения информационной безопасности»

Пример 1. Используя справочные средства операционной системы Windows найти и отобразить с экспортом в Microsoft Word:

1) понятия учетной записи и домена и типов доступа к операционной системе: глобальные, локальные, ограниченные и административные.

2) описание порядка создания, изменения, активации и удаления учетных записей.

3) основные категории локальных пользователей (пользователи и группы) и конкретных прав каждого вида учетных записей, включая администраторов, пользователей, опытных пользователей, операторов архива, репликаторов и гостей.

Пример 2. Используя средства Internet (kaspersky.ru и т.п.), справочные средства и антивирусное программное обеспечение:

1) найти и отобразить с экспортом в Microsoft Word понятия мошеннического программного обеспечения, хакерских атак, фишинга и спама.

2) найти и отобразить с экспортом в Microsoft Word описание порядка использования и ключевых функций Kaspersky Unlocker и Kaspersky Internet Security, дать сравнительную характеристику ключевых функций Kaspersky Rescue Disk и Kaspersky Antivirus (Kaspersky Virusscanner, Kaspersky Virus Removal Tool и т.д.).

3) открыть антивирусную программу, произвести настройку параметров ее работы, запустить проверку и сформировать отчет о результатах работы.

Пример 3.

1. Зашифровать следующие сообщения методом перестановки:
   ИНФОРМАЦИОННЫЕ СИСТЕМЫ
   ТЕЛЕКОММУНИКАЦИИ.
2. Зашифровать следующие сообщения методом подстановки:
   КОНФИДЕНЦИАЛЬНОСТЬ
   ШИФРОВАНИЕ
   КРИПТОГРАФИЯ
3. Расшифровать следующее сообщение методом перестановки без ключа:
   ЕЫНЬЛАНОСРЕП НАДЕЫН

Пример 4. Используя средства Internet и справочные средства программ резервного копирования найти и отобразить с экспортом в Microsoft Word:

1) понятия полного, дифференциального и инкрементного резервного копирования.

2) описание порядка создания образа и восстановления из него.

3) дать сравнительную характеристику основных функций трех программ резервного копирования по следующим критериям: условия распространения, планирование (работа по расписанию), возможности работы с разделами диска, создания загрузочного диска, шифрования, сжатия, настройки фильтров, онлайн резервного копирования.

Пример задания по теме 3. «Информационная безопасность в профессиональной деятельности»

Использование сетевых сервисов Веб 2.0.

1. Создание ментальной карты (https:// www.mindmup.com) на тему: «Виды вредоносных программ и методы защиты от них», «Защита цифровых коммуникаций», «Рекомендации по защите компании в сфере рекламы и СО» и др.

2. Создание вебмикса (https:// www.symbaloo.com) для реализации проекта «Интернет: проблемы защиты интеллектуальной собственности» и др..

3. Использование сервиса ленты времени (https:// www.sutori.com) по истории развития компьютерных вирусов.

2) Вопросы для устного опроса

Устный опрос № 1.

Тема 1. Законодательный и нормативно-правовой уровни обеспечения информационной безопасности

1. Понятие информационной безопасности
2. Субъекты и объекты информационной безопасности
3. Понятие и функции системы защиты информации
4. Общие принципы обеспечения информационной безопасности
5. Специальные принципы обеспечения информационной безопасности
6. Обеспечивающие подсистемы защиты информации
7. Нормативно-правовые основы информационной безопасности
8. Понятие информационной угрозы
9. Причины реализации информационных угроз
10. Виды реализации угроз информационной безопасности
11. Классификация информационных угроз
12. Способы воздействия информационных угроз
13. Прогресс информационных технологий и необходимость обеспечения
14. безопасности
15. Основные понятия информатизации общества и информационной безопасности
16. Структура понятия «Информационная безопасность»
17. Субъекты и объекты информационной безопасности
18. Нормативно-правовое регулирование информационной безопасности
19. Стандарты и спецификации в области информационной безопасности.
20. Типы международных организаций в сфере информационной безопасности
21. Направления работы крупных альянсов в сфере информационной безопасности
22. Понятие и особенности экономической информации как объекта безопасности
23. Перечень сведений, относящихся к коммерческой тайне
24. Перечень сведений, которые не могут составлять коммерческую тайну
25. Объекты банковской тайны
26. Статьи Уголовного кодекса о компьютерных преступлениях
27. Доктрина информационной безопасности РФ
28. Федеральный закон от №149-ФЗ «Об информации, информационных технологиях и о защите информации»
29. Федеральный закон от №63-ФЗ «Об электронной подписи»
30. Принципиальные подходы к обеспечению информационной безопасности

31. Сравнительная характеристика фрагментного и комплексного подхода к защите

32. информации

33. Общие принципы обеспечения информационной безопасности

34. Специфические методы обеспечения информационной безопасности

35. Принципы построения системы информационной безопасности

36. Системный подход к защите информации

37. Требования к системе мер защиты информации

38. Принципы построения и особенности практической реализации системы защиты информации экономического субъекта

39. Механизм обеспечения информационной безопасности РФ в сфере экономики

40. Цели, задачи и функции системы защиты информации

41. Обеспечивающие компоненты системы защиты информации

42. Методы и средства обеспечения информационной безопасности

43. Российское и международное законодательство в области защиты прав на интеллектуальную собственность.

44. Анализ рисков информационной безопасности.

Устный опрос № 2.

Тема 2. Программно-технические меры обеспечения информационной безопасности

1. Классификация вредоносного программного обеспечения
2. Классификация компьютерных преступлений
3. Методы обеспечения информационной безопасности
4. Средства обеспечения информационной безопасности
5. Криптографическое обеспечение информационной безопасности
6. Организационное обеспечение информационной безопасности
7. Особенности и этапы построения системы защиты информации
8. Методы реализации механизмов защиты информации
9. План построения системы защиты информации
10. Функции службы информационной безопасности
11. Симметричные криптосистемы. AES. ГОСТ.
12. Ассиметричные криптосистемы. RSA. El Gamal.
13. Криптографические протоколы. Общие понятия, типы криптопротоколов.
14. Протоколы аутентификации. Слабости парольных протоколов аутентификации. Виды атак и угроз для протоколов аутентификации. Полнота, корректность. Стойкость протокола.
15. Протокол аутентификации Фейге – Фиата - Шамира. Анализ протокола.
16. Протокол аутентификации Шнорра. Анализ протокола. Рекомендации по использованию. Сфера применения протокола.
17. Протоколы электронной подписи. Общие понятия и определения. Виды атак и угроз для протоколов электронной подписи. Стойкость протокола.

18. Криптографические хэш-функции. Определение и требования к ним. Задача вычисления коллизий хэш-функций. Атаки и угрозы для хэш-функций, стойкость хэш-функции. Области применения хэш-функций.
19. Хэш-функция SHA. Построение хэш-функций на основе стойких криптосистем.
20. Использование хэш-функций в протоколах электронной подписи. Протокол электронной подписи DSS.
21. Электронная подпись в системе RSA.
22. Архитектура системы безопасности ОС Windows.
23. Архитектура системы безопасности ОС Windows
24. Субъект доступа.
25. Объект доступа.
26. Механизм контроля доступа.
27. Диспетчер учётных записей SAM. Пароли и ключи пользователей.
28. База учётных записей SAM: типичные атаки и методы её защиты.
29. Введение в файловую систему NTFS. Права доступа стандартные, специфичные и родовые.
30. Разрешения NTFS индивидуальные, стандартные и специальные.
31. Механизм наследования разрешений. Средства редактирования разрешения NTFS.
32. Шифрование данных в NTFS. Рекомендации по защите средствами NTFS.
33. Безопасность сервера SMB. Введение в протокол SMB
34. Типичные атаки на протокол и методы защиты. Аудит сервера SMB.
35. Проверка подлинности при входе в домен Windows.
36. Защита реестра Windows.
37. Безопасность серверов RAS и IIS.
38. Инфраструктура открытых ключей PKI
39. Протокол KERBEROS
40. Криптоинтерфейс, криптопровайдеры
41. Защищенные протоколы и защищенные компьютерные системы
42. Удаленные атаки на защищенные компьютерные системы и методы защиты от них.

3) Примерный перечень вопросов, выносимых на зачет

1. Нормативно-правовое регулирование информационной безопасности.
2. Типы международных организаций в сфере информационной безопасности.
3. Статьи Уголовного кодекса о компьютерных преступлениях.
4. Доктрина информационной безопасности РФ.
5. Федеральный закон от №149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Федеральный закон от №63-ФЗ «Об электронной подписи».
7. Принципиальные подходы к обеспечению информационной безопасности.
8. Общие принципы обеспечения информационной безопасности.

9. Требования к системе мер защиты информации.
10. Принципы построения и особенности практической реализации системы защиты информации компании по рекламе и связям с общественностью.
11. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
12. Защита интеллектуальной собственности средствами патентного и авторского права.
13. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
14. Симметричные шифры.
15. Ассиметричные шифры.
16. Криптографические протоколы.
17. Криптографические хеш-функции.
18. Электронная подпись.
19. Служба безопасности организации в сфере рекламы СО.
20. Организационно-административные мероприятия обеспечения информационной безопасности в подразделениях компании по рекламе и СО.
21. Принципы обеспечения информационной безопасности на основе инженерно-технического обеспечения в компаниях по рекламе и СО.
22. Информационные угрозы и их классификация.
23. Действия и события, нарушающие информационную безопасность.
24. Основные виды каналов утечки информации.
25. Пути несанкционированного доступа к информации.
26. Стратегия и тактика злоумышленника при несанкционированном доступе.
27. Личностно - профессиональные характеристики сотрудников, способствующие реализации информационных угроз.
28. Способы воздействия угроз на информационные объекты.
29. Вредоносные программы, их виды.
30. Признаки воздействия вирусов на компьютерную систему.
31. Этапы построения системы защиты информации
32. Структура и функции службы информационной безопасности компании по рекламе и СО.
33. Оценка эффективности инвестиций в информационную безопасность
34. Методика защиты электронной почты
35. Электронная цифровая подпись и особенности ее применения
36. Защита информации в Интернете
37. Информационная безопасность пользователей мобильных устройств
38. Методы защиты цифровых коммуникаций.

6.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенций по дисциплине применяется традиционная система контроля и оценки успеваемости студентов.

При использовании традиционной системы контроля и оценки успеваемости студентов представлены критерии выставления оценок: «зачтено», «не зачтено».

Промежуточный контроль знаний проводится в форме зачета.

Критерии оценки зачёта представлены в таблице 7.

Таблица 7

Критерии выставления оценок на зачете

Оценка	Критерии оценивания
Зачтено	**«Зачтено»** выставляется, если студент самостоятельно и полностью использует возможности программных средств для решения прикладных задач; самостоятельно подтверждает ответ конкретными примерами; правильно и обстоятельно отвечает на дополнительные вопросы преподавателя; умеет пользоваться справочной литературой, поиском информации, раздаточным материалом.
Не зачтено	**«Не зачтено»** выставляется, если студент не может использовать программные средства при решении задач; не может подтвердить ответ конкретными примерами; не отвечает на большую часть дополнительных вопросов преподавателя; не может самостоятельно использовать справочную литературу, раздаточный материал, поиск информации.

7. Учебно-методическое и информационное обеспечение дисциплины

7.1 Основная литература

1. Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. – 5-е изд., стер. – Санкт-Петербург: Лань, 2019. – 324 с. – ISBN 978-5-8114-4067-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/114688 (открытый доступ).

2. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум: учебное пособие / Р. Н. Гилязова. – Санкт-Петербург: Лань, 2020. – 44 с. – ISBN 978-5-8114-4294-2. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/130179 (открытый доступ).

3. Информационная безопасность: учебное пособие / составители Е. Р. Кирколуп [и др.]. – Барнаул: АлтГПУ, 2017. – 316 с. – ISBN 978-5-88210-898-3. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/112164 (открытый доступ).

7.2 Дополнительная литература

1. Карпычев, В.Ю. Техническая защита информации. Каналы утечки информации: учебное пособие/ В.Ю. Карпычев, М. А. Степаненко, О. П. Тимофеева. – Нижний Новгород, 2018. – 92 с.

2. Гнездилова, Елена Валерьевна. Организация работы отделов рекламы и связей с общественностью: учебное пособие / Е. В. Гнездилова; Российский государственный аграрный университет - МСХА имени К. А. Тимирязева (Москва). – Электрон. текстовые дан. – Москва: РГАУ-МСХА им. К. А. Тимирязева, 2019 – 129 с. – Коллекция: Учебная и учебно-методическая литература. – Режим доступа: http://elib.timacad.ru/dl/local/umo410.pdf. – Загл. с титул. экрана. – https://doi.org/10.34677/2019.025. RL:http://elib.timacad.ru/dl/local/umo410.pdf.

3. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений: учебное пособие / С. Н. Никифоров. – 2-е изд., стер. – Санкт-Петербург: Лань, 2019. – 96 с. – ISBN 978-5-8114-4040-5. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/114697 (открытый доступ).

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

1. Бесплатное дистанционное обучение в Национальном Открытом Университете «ИНТУИТ» [Электронный ресурс]. – Режим доступа: http://www.intuit.ru (открытый доступ).

2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ Шаньгин В.Ф. – Электрон. Текстовые данные. – Саратов: Профобразование, 2017. – 544 с. – Режим доступа: http://www.iprbookshop.ru/63592.html (открытый доступ)

9. Перечень программного обеспечения и информационных справочных систем

1. 1 Справочная правовая система «КонсультантПлюс» (открытый доступ): [Электронный ресурс]. – Режим доступа: www.consultant.ru. – Загл. с экрана.

Таблица 8

Перечень программного обеспечения

Наименование темы учебной дисциплины	Наименование программы	Тип программы	Автор	Год разработки
По всем темам дисциплины	Microsoft Windows 7 и выше	Операционная система	Microsoft	2009
	Microsoft Office 2010 и выше	Пакет офисных программ		2010
	Google Chrome	Браузер		2012

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения лекционных и практических занятий по дисциплине «Информационная безопасность и безопасность профессиональной деятельности» необходимы аудитория и компьютерный класс, подключенные к сети Интернет, оснащенные средствами мультимедиа и программными средствами: MS Windows 7/8/10; MS Office 2007/2010/2013/365 (Office Online), системой КонсультантПлюс, программой демонстрации NetOp School, браузером Google Chrome.

Лекции проводятся в специализированной аудитории, оборудованной мультимедийным проектором для демонстрации компьютерных презентаций.

Для проведения практических занятий по дисциплине «Информационная безопасность и безопасность профессиональной деятельности» необходим компьютерный класс с установленными на ПК программным обеспечением, указанным в п. 9.

Таблица 9

Сведения об обеспеченности специализированными аудиториями, кабинетами, лабораториями

Наименование специальных помещений и помещений для самостоятельной работы (№ учебного корпуса, № аудитории)	Оснащенность специальных помещений и помещений для самостоятельной работы
1	2
Аудитория для проведения занятий лекционного типа № 118 - уч. корпус № 15	Видеопроектор 3500 Лм
Аудитория для проведения практических занятий №УИТ-113, уч. корпус №15	Персональные компьютеры в количестве 20 штук
Аудитория для проведения практических занятий №УИТ-110, уч. корпус №15	Персональные компьютеры в количестве 20 штук
Аудитория для проведения практических занятий №УИТ-114, уч. корпус №15	Персональные компьютеры (терминалы) в количестве 20 штук
Аудитория для проведения практических занятий №УИТ-102, уч. корпус №15	Персональные компьютеры (терминалы) в количестве 20 штук
Центральная научная библиотека имени Н.И. Железнова	Читальные залы библиотеки
Общежитие	Комната для самоподготовки

11. Методические рекомендации студентам по освоению дисциплины

Изучение учебной дисциплины «Информационная безопасность и безопасность профессиональной деятельности» включает освоение материалов лекций, приобретение практических навыков работы с программными средствами.

На лекциях при помощи мультимедиа проектора и презентаций раскрываются основные теоретические вопросы дисциплины, делаются акценты на наиболее сложные положения изучаемого материала.

Лекционный материал следует просматривать и изучать по конспекту/электронной презентации самостоятельно после аудиторных занятий. Для более углубленного изучения материала необходимо использовать рекомендованную литературу и Интернет-ресурсы.

Практические занятия проводятся в компьютерных классах с применением методических материалов. На занятиях необходимо иметь электронный носитель информации – флэш-карту для сохранения результатов своей работы. Учебные материалы можно сохранять в облачных сервисах: Google Диск, Яндекс.Диск, Облако Mail.Ru, Dropbox.

Посещение лекций и практических занятий – обязательно.

Консультирование по выполнению заданий практических работ проводится в компьютерных классах во время консультаций по графику (см. на стендах кафедры), а также через электронный обмен сообщениями с преподавателями, посредством Интернет и электронной информационно-образовательной среды Университета через личный кабинет.

Необходимо соблюдать сроки выполнения всех заданий.

Полученные оценки за выполненные задания являются основой для промежуточной аттестации.

Виды и формы отработки пропущенных занятий

Магистр, обязан отработать:

- пропущенные лекции – представив преподавателю конспект лекции, ответив на вопросы устно;
- пропущенные практические занятия – в форме выполнения заданий, устного опроса, посещения дополнительных занятий.

12. Методические рекомендации преподавателям по организации обучения по дисциплине

Учебный процесс по курсу «Информационная безопасность и безопасность профессиональной деятельности» включает следующие организационные формы: лекции, практические занятия и консультации, а также систему контроля знаний, самостоятельную работу студентов.

Методика чтения лекций зависит от цели и задач изучения предмета/раздела, а также уровня общей подготовки обучающихся, форма ее проведения – от характера темы и содержания материала. Высокая

эффективность деятельности преподавателя во время чтения лекции достигается за счет глубокого освоения предметной области, педагогического мастерства, высокой речевой культуры и ораторского искусства, когда учитывается психология аудитории, закономерности восприятия, внимания, мышления, эмоциональные процессы учащихся, обратная связь и принципы дидактики.

При подготовке материала лекции преподавателю необходимо:

– учитывать требования государственного образовательного стандарта, учебного плана и рабочей программы;

– применять принципы дидактики (наглядность, от теории к практике, доступность, структуризация и систематизация и т.д.);

– уметь создавать интерактивные презентации;

– уметь использовать технические (проектор) и программные средства (например, программу подготовки презентаций MS PowerPoint, программу управления компьютерным классом NetOp School) и др.

Для проведения практических занятий преподавателю следует разрабатывать задания различной степени сложности, инструкции (методические указания) по выполнению каждого задания, раздаточный материал в печатном и электронном виде.

По курсу «Информационная безопасность и безопасность профессиональной деятельности» должны быть организованы:

– «очные» консультации в компьютерном классе, проводимые преподавателем согласно графику (размещается на стендах кафедры);

– off-line консультации, проводимые преподавателем с помощью электронной почты;

– взаимодействия в электронной информационно-образовательной среде Университета через личный кабинет.

Для организации контрольных мероприятий преподавателю следует подготовить вопросы для устного опроса и практические задания. Преподаватель должен использовать различные методы обучения:

– объяснительно-иллюстративный (лекция, объяснение, работа с учебником, демонстрация презентаций);

– репродуктивный (воспроизведение действий по применению знаний на практике, деятельность по алгоритму, программирование);

– частично-поисковый (поиск решения познавательных задач под руководством преподавателя);

– исследовательский метод, в котором после анализа материала, постановки проблем и задач и краткого устного или письменного инструктажа обучаемые самостоятельно изучают литературу, источники, ведут наблюдения и измерения и выполняют другие действия поискового характера.

– активные методы: групповое обсуждение, интерактивная лекция и др.

Программу разработали:

Лемешко Т.Б., ст. преподаватель _____

Худякова Е.В., д.э.н., профессор _____

РЕЦЕНЗИЯ

на рабочую программу дисциплины
Б1.В.11 «Информационная безопасность и
безопасность профессиональной деятельности»
ОПОП ВО по направлению 42.04.01 Реклама и связи с общественностью,
направленность «Реклама и связи с общественностью в отрасли (в сфере АПК)»
(квалификация выпускника – магистр)

Остапчук Татьяной Владимировной, доцентом кафедры бухгалтерского учета ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева, кандидатом экономических наук (далее по тексту рецензент) проведено рецензирование рабочей программы учебной дисциплины «Информационная безопасность и безопасность профессиональной деятельности» по направлению 42.04.01 Реклама и связи с общественностью, направленность «Реклама и связи с общественностью в отрасли (в сфере АПК)», разработанной в ФГБОУ ВО «Российский государственный аграрный университет – МСХА имени К.А. Тимирязева» на кафедре прикладной информатики (разработчики: Худякова Е.В., д.э.н., профессор и Лемешко Т.Б., ст. преподаватель).

Рассмотрев представленные на рецензирование материалы, рецензент пришел к следующим выводам:

1. Предъявленная рабочая программа дисциплины «Информационная безопасность и безопасность профессиональной деятельности» (далее по тексту Программа) *соответствует* требованиям ФГОС ВО по направлению 42.04.01 Реклама и связи с общественностью. Программа *содержит* все основные разделы, *соответствует* требованиям к нормативно-методическим документам.

2. Представленная в Программе ***актуальность*** учебной дисциплины в рамках реализации ОПОП ВО *не подлежит сомнению* – дисциплина включена в часть, формируемая участниками образовательных отношений учебного цикла – Б1.

3. Представленные в Программе ***цели*** дисциплины *соответствуют* требованиям ФГОС ВО направления 42.04.01 Реклама и связи с общественностью.

4. В соответствии с Программой за дисциплиной «Информационная безопасность и безопасность профессиональной деятельности» закреплены профессиональные компетенции (индикаторы): **ПКос-3.1; ПКос-1.1; ПКос-1.2**. Дисциплина «Информационная безопасность и безопасность профессиональной деятельности» и представленная Программа *способна реализовать* их в объявленных требованиях.

5. ***Результаты обучения***, представленные в Программе в категориях знать, уметь, владеть *соответствуют* специфике и содержанию дисциплины и *демонстрируют возможность* получения заявленных результатов.

6. Общая трудоёмкость дисциплины «Информационная безопасность и безопасность профессиональной деятельности» составляет 2 зачётных единицы (72 часа).

7. Информация о взаимосвязи изучаемых дисциплин и вопросам исключения дублирования в содержании дисциплин *соответствует* действительности. Дисциплина «Информационная безопасность и безопасность профессиональной деятельности» взаимосвязана с другими дисциплинами ОПОП ВО и Учебного плана по направлению 42.04.01 Реклама и связи с общественностью**.**

8. Представленная Программа предполагает использование современных образовательных технологий, используемые при реализации различных видов учебной работы. Формы образовательных технологий *соответствуют* специфике дисциплины.

9. Программа дисциплины «Информационная безопасность и безопасность профессиональной деятельности» предполагает проведение занятий в интерактивной форме.

10. Виды, содержание и трудоёмкость самостоятельной работы магистров, представленные в Программе, *соответствуют* требованиям к подготовке выпускников, содержащимся во ФГОС ВО направления 42.04.01 Реклама и связи с общественностью.

11. Представленные и описанные в Программе формы *текущей* оценки знаний *соответствуют* специфике дисциплины и требованиям к выпускникам.

Форма промежуточного контроля знаний магистров, предусмотренная Программой, осуществляется в форме зачёта, что соответствует статусу дисциплины, которая включена в часть, формируемая участниками образовательных отношений учебного цикла – Б1. ФГОС ВО направления 42.04.01 Реклама и связи с общественностью.

12. Формы оценки знаний, представленные в Программе, *соответствуют* специфике дисциплины и требованиям к выпускникам.

13. Учебно-методическое обеспечение дисциплины представлено: основной литературой – 3 источника, дополнительной литературой – 3 наименования, Интернет-ресурсы – 2 источника и *соответствует* требованиям ФГОС ВО направления 42.04.01 Реклама и связи с общественностью.

14. Материально-техническое обеспечение дисциплины соответствует специфике дисциплины «Информационная безопасность и безопасность профессиональной деятельности» и обеспечивает использование современных образовательных, в том числе интерактивных методов обучения.

15. Методические рекомендации магистрам и методические рекомендации преподавателям по организации обучения по дисциплине дают представление о специфике обучения по дисциплине «Информационная безопасность и безопасность профессиональной деятельности».

ОБЩИЕ ВЫВОДЫ

На основании проведенного рецензирования можно сделать заключение, что характер, структура и содержание рабочей программы дисциплины «Информационная безопасность и безопасность профессиональной деятельности» ОПОП ВО по направлению 42.04.01 Реклама и связи с общественностью, направленность «Реклама и связи с общественностью в отрасли (в сфере АПК)» (квалификация выпускника – магистр), разработанной Худяковой Е.В., д.э.н., профессором и Лемешко Т.Б.,ст. преподавателем кафедры прикладной информатики, соответствует требованиям ФГОС ВО, современным требованиям экономики, рынка труда и позволит при её реализации успешно обеспечить формирование заявленных компетенций.

Рецензент: Остапчук Т.В., доцент кафедры бухгалтерского учета ФГБОУ ВО РГАУ-МСХА имени К.А. Тимирязева, кандидат экономических наук

_____ «13» 01 2020 г.
(подпись)