Фонд оценочных средств для промежуточной аттестации

по дисциплине (модулю)
Информационная безопасность в работе СМИ (научный семинар)

Направление подготовки (специальность)
42.03.02 Журналистика

Направленность (профиль)
Производство медиапродукта на различных платформах

Присваиваемая квалификация
бакалавр

Форма обучения
очная

Челябинск 2025 г.

42.03.02 Журналистика, Производство медиапродукта на различных платформах, Информационная безопасность в работе СМИ (научный семинар), 2025, очная

Проректор по учебной работе утверждено 24.02.25 А.А.Саламатов

Ученым советом факультета журналистики

Протокол заседания № 8 от 10.02.2025

Председатель Ученого совета
факультета журналистики согласовано Б. Н. Киршин

Заседанием кафедры теории медиа

Протокол заседания № 7 от 06.02.2025

Заведующий кафедрой согласовано Е.Ю.Панова

Автор (составитель) М.А.Демчук

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13» апреля 2021 г. № 247-1

Содержание

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Направление подготовки: *42.03.02 «Журналистика»*
Направленность (профиль) Производство медиапродукта на различных платформах
Дисциплина: *Информационная безопасность в работе СМИ (научный семинар)*
Семестр (семестры) изучения: *6*
Форма (формы) промежуточной аттестации: *зачёт*

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ

Изучение дисциплины «Информационная безопасность в работе СМИ (научный семинар)» направлено на формирование следующих компетенций:

Коды компетенции согласно ФГОС (ОПОП ВО)	Содержание компетенций согласно ФГОС (ОПОП ВО)	Индикаторы достижения компетенции согласно ОПОП	Перечень планируемых результатов обучения по дисциплине
1	2	3	4
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Выполняет поиск информации, определяет критерии системного анализа поставленных задач УК-1.2 Использует критический анализ, систематизацию и обобщение информации для решения поставленных задач	**Знать** Для достижения УК-1.1: Знать основы поиска информации, определения критериев системного анализа поставленных задач **Уметь** Для достижения УК-1.1: Уметь выполнять поиск информации, определять критерии системного анализа поставленных задач **Владеть** Для достижения УК-1.1: Владеть навыками поиска информации, определения критериев системного анализа поставленных задач **Знать** Для достижения УК-1.2: Знать основы использования критического анализа, систематизации и обобщения информации для решения поставленных задач

			Уметь Для достижения УК-1.2: Уметь использовать критический анализ, систематизацию и обобщение информации для решения поставленных задач **Владеть** Для достижения УК-1.2: Владеть навыками критического анализа, систематизации и обобщения информации для решения поставленных задач
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1 Знать правила выявления и анализа различных способов решения задач в рамках цели проекта и аргументации их выбора УК-2.2 Уметь выявлять и анализировать различные способы решения задач в рамках цели проекта и аргументировать их выбор УК-2.3 Владеть навыками выявления и анализа различных способов решения задач в рамках цели проекта и аргументации их выбора	**Знать** Для достижения УК-2.1: Знать теоретические основы принятия решений в сфере управления проектами **Уметь** Для достижения УК-2.1: Уметь работать с теоретическими основами принятия решений в сфере управления проектами **Владеть** Для достижения УК-2.1: Владеть навыками использования теоретических основ принятия решений в сфере управления проектами **Знать** Для достижения УК-2.2: Знать правила выявления и анализа различных способов решения задач в рамках цели проекта и аргументации их выбора **Уметь** Для достижения УК-2.2: Уметь выявлять и анализировать различные способы решения задач в рамках цели проекта и аргументировать их выбор **Владеть** Для достижения УК-2.2: Владеть навыками выявления и анализа различных способов решения задач в рамках цели проекта и аргументации их выбора **Знать** Для достижения УК-2.3: Знать принципы составления и проведения социологических опросов

			Уметь Для достижения УК-2.3: Уметь проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений **Владеть** Для достижения УК-2.3: Владеть навыками проектирования решения конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений
ПК-2	Способен осуществлять редакторскую деятельность в соответствии с языковыми нормами, стандартами, форматами, жанрами, стилями, технологическими требованиями разных типов СМИ и других медиа	ПК-2.1 Приводит журналистский текст и (или) продукт разных видов в соответствие с языковыми нормами ПК-2.2 Контролирует соблюдение редакционных стандартов, форматов, жанров, стилей в журналистском тексте и (или) продукте ПК-2.3 Контролирует соблюдение профессиональных этических норм в журналистском тексте и (или) продукте ПК-2.4 Учитывает технологические требования разных типов СМИ и других медиа при редактировании журналистского текста и (или) продукта	**Знать** Для достижения ПК-2.1: Знать принципы обработки журналистского текста и (или) продукта разных видов в соответствие с языковыми нормами **Уметь** Для достижения ПК-2.1: Уметь применять принципы обработки журналистского текста и (или) продукта разных видов в соответствие с языковыми нормами **Владеть** Для достижения ПК-2.1: Владеть практическими навыками обработки журналистского текста и (или) продукта разных видов в соответствие с языковыми нормами **Знать** Для достижения ПК-2.2: Знать принципы соблюдения редакционных стандартов, форматов, жанров, стилей в журналистском тексте и (или) продукте **Уметь** Для достижения ПК-2.2: Уметь контролировать соблюдение редакционных стандартов, форматов, жанров, стилей в журналистском тексте и (или) продукте **Владеть** Для достижения ПК-2.2: Владеть практическими навыками

			использования стандартов, форматов, жанров, стилей в журналистском тексте и (или) продукте **Знать** Для достижения ПК-2.3: Знать профессиональные этические нормы в журналистском тексте и (или) продукте **Уметь** Для достижения ПК-2.3: Уметь применять профессиональные этические нормы в журналистском тексте и (или) продукте **Владеть** Для достижения ПК-2.3: Владеть практическим опытом применения профессиональных этических норм в журналистском тексте и (или) продукте **Знать** Для достижения ПК-2.4: Знать технологические требования разных типов СМИ и других медиа при редактировании журналистского текста и (или) продукта **Уметь** Для достижения ПК-2.4: Уметь применять технологические требования разных типов СМИ и других медиа при редактировании журналистского текста и (или) продукта **Владеть** Для достижения ПК-2.4: Владеть практическим опытом применения технологических требований разных типов СМИ и других медиа при редактировании журналистского текста и (или) продукта

3. СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

3.1 Виды оценочных средств

№ п/п	Код компетенции/ планируемые результаты обучения	Контролируемые темы/ разделы	Наименование оценочного средства для текущего контроля	Наименование оценочного средства на промежуточной аттестации/№ задания
1	УК-1 **Знать** Для достижения УК-1.1: Знать основы поиска информации, определения критериев системного анализа поставленных задач **Уметь** Для достижения УК-1.1: Уметь выполнять поиск информации, определять критерии системного анализа поставленных задач **Владеть** Для достижения УК-1.1: Владеть навыками поиска информации, определения критериев системного анализа поставленных задач **Знать** Для достижения УК-1.2: Знать основы использования критического анализа, систематизации и обобщения информации для решения поставленных задач **Уметь** Для достижения УК-1.2: Уметь использовать критический анализ, систематизацию и обобщение информации для решения поставленных задач **Владеть** Для достижения УК-1.2: Владеть навыками критического анализа, систематизации и обобщения информации для решения поставленных задач	1. Место информационной безопасности в национальной безопасности РФ. 2. Составляющие информационной безопасности. 3. Виды и источники угроз информационной безопасности РФ. 4. Информационные риски в работе печатных и сетевых СМИ. 5. Схема воздействия угроз на информационную повестку. 6. Перспективные направления в области информационной безопасности.	1. Творческое задание.	1. Вопросы к зачёту.

2	УК-2 **Знать** Для достижения УК-2.1: Знать теоретические основы принятия решений в сфере управления проектами **Уметь** Для достижения УК-2.1: Уметь работать с теоретическими основами принятия решений в сфере управления проектами **Владеть** Для достижения УК-2.1: Владеть навыками использования теоретических основ принятия решений в сфере управления проектами **Знать** Для достижения УК-2.2: Знать правила выявления и анализа различных способов решения задач в рамках цели проекта и аргументации их выбора **Уметь** Для достижения УК-2.2: Уметь выявлять и анализировать различные способы решения задач в рамках цели проекта и аргументировать их выбор **Владеть** Для достижения УК-2.2: Владеть навыками выявления и анализа различных способов решения задач в рамках цели	1. Место информационной безопасности в национальной безопасности РФ. 2. Составляющие информационной безопасности. 3. Виды и источники угроз информационной безопасности РФ. 4. Информационные риски в работе печатных и сетевых СМИ. 5. Схема воздействия угроз на информационную повестку. 6. Перспективные направления в области информационной безопасности.	1. Творческое задание.	1. Вопросы к зачёту.

	проекта и аргументации их выбора **Знать** Для достижения УК-2.3: Знать принципы составления и проведения социологических опросов **Уметь** Для достижения УК-2.3: Уметь проектировать решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений **Владеть** Для достижения УК-2.3: Владеть навыками проектирования решения конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений			
3	ПК-2 **Знать** Для достижения ПК-2.1: Знать принципы обработки журналистского текста и (или) продукта разных видов в соответствие с языковыми нормами **Уметь** Для достижения ПК-2.1: Уметь применять принципы обработки журналистского текста и (или) продукта разных видов в соответствие с языковыми нормами **Владеть** Для достижения ПК-2.1: Владеть практическими навыками обработки журналистского текста и (или) продукта разных видов в соответствие с языковыми нормами **Знать**	1. Место информационной безопасности в национальной безопасности РФ. 2. Составляющие информационной безопасности. 3. Виды и источники угроз информационной безопасности РФ. 4. Информационные риски в работе печатных и сетевых СМИ. 5. Схема воздействия угроз на информационную повестку. 6. Перспективные направления в области информационной безопасности.	1. Творческое задание.	1. Вопросы к зачёту.

	Для достижения ПК-2.2: Знать принципы соблюдения редакционных стандартов, форматов, жанров, стилей в журналистском тексте и (или) продукте **Уметь** Для достижения ПК-2.2: Уметь контролировать соблюдение редакционных стандартов, форматов, жанров, стилей в журналистском тексте и (или) продукте **Владеть** Для достижения ПК-2.2: Владеть практическими навыками использования стандартов, форматов, жанров, стилей в журналистском тексте и (или) продукте **Знать** Для достижения ПК-2.3: Знать профессиональные этические нормы в журналистском тексте и (или) продукте **Уметь** Для достижения ПК-2.3: Уметь применять профессиональные этические нормы в журналистском тексте и (или) продукте **Владеть** Для достижения ПК-2.3: Владеть практическим опытом применения профессиональных этических норм в журналистском тексте и (или) продукте **Знать** Для достижения ПК-2.4: Знать технологические требования разных типов СМИ и других медиа при редактировании журналистского текста и (или) продукта **Уметь**			

	Для достижения ПК-2.4: Уметь применять технологические требования разных типов СМИ и других медиа при редактировании журналистского текста и (или) продукта **Владеть** Для достижения ПК-2.4: Владеть практическим опытом применения технологических требований разных типов СМИ и других медиа при редактировании журналистского текста и (или) продукта			

Типовые задания, критерии и показатели оценивания в рамках текущего контроля представлены в рабочей программе дисциплины (модуля). Полные комплекты оценочных средств и контрольно-измерительных материалов хранятся на кафедре.

3.2 Содержание оценочных средств

Пример творческого задания (с кратким ответом):

1. Привести примеры соблюдения информационной безопасности в работе печатных и сетевых СМИ (примеры берутся из публикаций, вышедших в свет не ранее чем месяц назад).

Анализируя текущий медийный ландшафт, можно выделить несколько ярких примеров того, как редакции осознанно подходят к вопросам информационной безопасности, выходя далеко за рамки простой проверки фактов. Речь идет о защите как самих источников и героев публикаций, так и аудитории от потенциально вредоносного контента.

Один из наглядных примеров – это **работа с данными граждан-жертв чрезвычайных происшествий**. В конце сентября 2024 года в ряде СМИ, например, в публикациях «Коммерсанта» и РИА «Новости» о пожаре в многоэтажном доме, можно было наблюдать строгое соблюдение этических и security-норм. Журналисты не публиковали имена погибших до официального подтверждения и информирования родственников, избегали показа шокирующих кадров с места событий, которые могли бы нанести психологическую травму аудитории, и использовали размытие лиц на фотографиях случайных свидетелей, не давших согласия на съемку. Это классический пример защиты приватности и нераспространения непроверенной или травмирующей информации.

Другой пример связан с **освещением тем, связанных с кибербезопасностью и хакерскими атаками**. В начале октября сетевое издание «Хакер» (часть медиахолдинга Rambler&Co) опубликовало материал о новой фишинговой схеме, нацеленной на

пользователей банковских приложений. Вместо того чтобы давать пошаговую инструкцию для злоумышленников, журналисты сосредоточились на детальном объяснении механизма мошенничества для рядовых пользователей, перечислили четкие признаки угрозы и дали инструкции по защите (не переходить по подозрительным ссылкам, проверять адреса сайтов и т.д.). Таким образом, СМИ выступило здесь не как распространитель опасных знаний, а как просветительский ресурс, повышающий цифровую грамотность и реально обеспечивающий безопасность своей аудитории.

Третий пример – это **работа с источниками в чувствительных политических или коррупционных расследованиях**. Хотя конкретные тексты могут быть закрыты платным доступом или опубликованы в нишевых изданиях, общая практика такова: журналисты все чаще используют сквозное шифрование для переписки с информаторами (мессенджеры Signal, Telegram с секретными чатами), обезличивают передаваемые массивы данных (метаданные, имена), а в самом тексте используют формулировки вроде «по словам источника, близкого к администрации президента», чтобы сделать идентификацию человека невозможной. Это прямая операционная безопасность (OpSec) в действии, направленная на защиту конфиденциальности и самих источников, и журналистов.

2. Каким образом организуется работа редакций печатных и сетевых СМИ в плане соблюдения информационной безопасности?

Организация работы редакции в сфере информационной безопасности – это сложный, многоуровневый процесс, который интегрирован как в ежедневные рутины, так и в стратегическое управление. Его можно разделить на несколько ключевых блоков.

Во-первых, это **нормативно-процедурный блок**. Крупные редакции разрабатывают и внедряют внутренние регламенты и редакционные политики. В этих документах четко прописаны: правила верификации информации (обязательное подтверждение из двух независимых источников, работа с первоисточниками, а не новостными агрегаторами), правила общения с источниками (когда можно обещать анонимность, как хранить контакты), этические кодексы по работе с жертвами насилия, детьми и в кризисных ситуациях. Например, в редакции «Коммерсанта» или «Медузы» существует институт юристов, которые проверяют материалы на предмет соответствия законодательству (например, о клевете, экстремизме, разглашении гостайны) до публикации.

Во-вторых, это **технический блок**. Редакции инвестируют в защищенную IT-инфраструктуру: используют VPN, средства защиты от DDoS-атак для своих сайтов, корпоративные почты с двухфакторной аутентификацией, системы безопасного удаленного доступа к материалам для журналистов. Файлы с конфиденциальными данными и черновики расследований хранятся в зашифрованных облачных хранилищах или на изолированных серверах. Проводятся регулярные тренинги для сотрудников по распознаванию фишинговых писем и социальной инженерии.

В-третьих, это **организационно-ролевой блок**. Ответственность за ИБ распределяется по вертикали. Шеф-редактор или главный редактор несет общую ответственность. Выпускающие редакторы проверяют каждый материал на соответствие стандартам безопасности и этики. Ответственный за соцсети следит за тем, чтобы в

публикациях не было утечек персональных данных или непроверенных слухов. В крупных холдингах есть отделы кибербезопасности, которые работают на опережение, мониторя угрозы для инфраструктуры издания в целом. Таким образом, ИБ становится не дополнительной обязанностью, а вшитым элементом каждого этапа создания новостного продукта.

3. Риски нарушения информационной безопасности в работе редакций печатных и сетевых СМИ.

Риски, с которыми сталкиваются современные СМИ, крайне разнообразны и могут иметь катастрофические последствия как для репутации издания, так и для физической безопасности его сотрудников и источников.

1. **Репутационные и юридические риски.** Самый частый риск – публикация непроверенной или ложной информации (фейк-ньюс), что ведет к потере доверия аудитории, судебным искам о защите чести и достоинства, а в случае с государственными СМИ – к подрыву авторитета власти. Сюда же относится несоблюдение авторских прав и плагиат, что влечет за собой финансовые потери и санкции.
2. **Риски для физической и психологической безопасности.** При освещении военных конфликтов, террористических актов или работы в «горячих точках» некорректная информация (например, точное расположение военных объектов) может быть использована противником и привести к человеческим жертвам. Неосторожная работа с данными жертв или свидетелей преступлений может сделать их мишенью для мести. Для самих журналистов разглашение маршрутов или местоположения в зоне конфликта – прямая угроза жизни.
3. **Операционные и киберриски.** Это хакерские атаки на сайты и инфраструктуру СМИ с целью их вывода из строя (DDoS), похищения конфиденциальных данных (взлом облачных хранилищ с готовящимися расследованиями), компрометации корпоративной переписки. Например, утечка переписки редакции может раскрыть внутренние источники или планы публикаций, нанеся непоправимый ущерб.
4. **Риски, связанные с источниками информации.** Нарушение договоренностей об анонимности, случайная или намеренная деанонимизация источника в тексте или метаданных файла может разрушить карьеру человека, подвергнуть его преследованиям по статье 144 УК РФ («Воспрепятствование законной профессиональной деятельности журналистов») или более серьезным обвинениям. Это не только трагедия для самого источника, но и подрыв доверия ко всему журналистскому сообществу, которое лишается важных каналов информации.
5. **Манипулятивные риски.** СМИ может невольно стать инструментом в информационной войне, манипулируя общественным мнением через специально поданные вбросы или нарративы. Это подрывает информационный суверенитет и стабильность в обществе, а для самого издания оборачивается потерей объективности и превращением в пропагандистский ресурс.

Таким образом, информационная безопасность для СМИ – это не просто

технический протокол, а комплексная стратегия выживания, сохранения репутации и выполнения своей фундаментальной общественной миссии в цифровую эпоху.

Вопросы зачёта (с краткими ответами):

1. Место информационной безопасности в национальной безопасности РФ.

В современную эпоху информационная безопасность (ИБ) перестала быть узкотехнической задачей и превратилась в один из краеугольных камней всей системы национальной безопасности Российской Федерации. Это положение закреплено стратегически – в Стратегии национальной безопасности РФ и, что еще важнее, в Доктрине информационной безопасности. Место ИБ определяется тем, что информационная сфера сегодня пронизывает все без исключения области жизни государства: оборону, экономику, науку, технологическое развитие, общественную стабильность и государственное управление. Таким образом, угрозы в информационной сфере напрямую подрывают суверенитет, территориальную целостность и конституционный строй страны. Например, кампания по дезинформации может спровоцировать социальную рознь, а кибератака на критическую инфраструктуру (энергетику, финансы) способна парализовать жизнедеятельность целых регионов. Поэтому обеспечение информационной безопасности является не просто составной частью, а необходимым условием и фундаментом для гарантирования национальной безопасности в целом.

2. Составляющие информационной безопасности.

Информационная безопасность как комплексная система опирается на несколько ключевых составляющих, часто называемых принципами или свойствами. Классическая триада, известная как «CIA» (Confidentiality, Integrity, Availability), включает в себя:

Конфиденциальность: это обеспечение доступа к информации только для authorized пользователей (лиц, систем, процессов). Проще говоря, информация не должна стать известной тем, кто не имеет на нее права. Это достигается через шифрование, разграничение прав доступа, политики паролей.

Целостность: это гарантия точности и полноты информации, а также защиты от несанкционированного изменения или уничтожения. Важно, чтобы данные не были искажены случайно или умышленно. Механизмы контроля целостности включают хеширование, электронную цифровую подпись (ЭЦП).

Доступность: это обеспечение доступа к информации и связанным с ней активам для санкционированных пользователей тогда, когда это необходимо. Даже самая защищенная информация бесполезна, если к ней нельзя получить доступ в нужный момент. Угрозой доступности являются, например, DDoS-атаки.

Помимо этой классической триады, часто добавляют и другие составляющие, такие как **аутентичность** (подтверждение подлинности автора информации и самой

информации), **подотчетность** (невозможность отказа от совершенных действий) и **достоверность** (соответствие информации реальному положению дел).

3. Виды и источники угроз информационной безопасности РФ.

Угрозы информационной безопасности России носят многообразный и комплексный характер. По своему **виду** их можно разделить на:

Политико-идеологические: целенаправленное воздействие на общественное сознание с целью подрыва доверия к органам власти, разжигания социальной, расовой, национальной розни, манипулирования общественным мнением.

Экономические: промышленный шпионаж, хищение интеллектуальной собственности, вывод из строя банковских систем, дестабилизация финансового рынка.

Криминальные: действия киберпреступников с целью вымогательства (с использованием ransomware), кражи персональных и платежных данных.

Техногенные и природные: сбои в работе информационной инфраструктуры из-за аварий, катастроф или стихийных бедствий.

Источники этих угроз также разнообразны:

Внешние: разведывательные службы иностранных государств, транснациональные преступные группировки, зарубежные хактивистские группировки, структуры, ведущие информационно-психологическую войну.

Внутренние: недобросовестные конкуренты, коррумпированные сотрудники, инсайдеры, представители экстремистских организаций внутри страны.

Стихийные: недостаточный уровень технологической независимости России в области IT, "человеческий фактор" (ошибки сотрудников, низкая грамотность в области ИБ).

4. Информационные риски в работе редакций печатных и сетевых СМИ.

Редакции СМИ работают в эпицентре информационного поля, что порождает для них специфические и высокие риски.

Риск публикации недостоверной информации (фейков): самый очевидный риск. Непроверенная информация подрывает репутацию СМИ как достоверного источника, может спровоцировать панику или общественные беспорядки, а также привести к судебным искам о защите чести и достоинства.

Риск нарушения конфиденциальности источников: утечка данных журналистского расследования, раскрывающая конфиденциального информатора, ставит под угрозу его безопасность и разрушает доверие ко всему журналистскому сообществу.

Риск кибератак на инфраструктуру редакции: взлом сайта, корпоративной почты или облачного хранилища может привести к уничтожению или хищению готовящихся материалов, компрометации внутренней переписки, подмене контента (дефейсинг) для распространения ложной информации от имени издания.

Риск непреднамеренного разглашения конфиденциальных данных: в публикации или в метаданных медиафайла (например, фотографии) могут остаться скрытые сведения (геолокация, имена, технические параметры), раскрывающие

местоположение героя или детали операции.

Риск нарушения законодательства: публикация материалов, разжигающих ненависть, разглашающих государственную или коммерческую тайну, нарушающих авторские права, влечет за собой административную и уголовную ответственность.

5. Схема воздействия угроз на информационную систему.

Воздействие угрозы на информационную систему можно представить в виде последовательной схемы, описывающей этапы кибератаки (киберубийцы). Классической моделью является модель Lockheed Martin «Cyber Kill Chain»:

1. **Разведка (Reconnaissance):** злоумышленник собирает информацию о цели (сетевые адреса, сотрудники, используемое ПО).
2. **Создание оружия (Weaponization):** подготовка вредоносного инструмента, например, создание файла с эксплойтом, прикрепленного к фишинговому письму.
3. **Доставка (Delivery):** Передача вредоносного средства цели (по электронной почте, через USB-носитель, через уязвимость на веб-сайте).
4. **Эксплуатация (Exploitation):** активация кода, использующего уязвимость в системе жертвы.
5. **Установка (Installation):** установка на систему жертвы backdoor'a или иного вредоносного ПО, обеспечивающего постоянный доступ.
6. **Установление командования и управления (Command and Control – C2):** зараженная система выходит на связь с сервером злоумышленника для получения инструкций.
7. **Действия по достижению цели (Actions on Objectives):** финальная стадия, на которой злоумышленник выполняет свою цель: шифрует данные для выкупа, похищает информацию, разрушает систему.

6. Перспективные направления в области информационной безопасности.

Сфера ИБ динамично развивается, и среди наиболее перспективных направлений можно выделить:

Искусственный интеллект и машинное обучение (AI/ML): использование AI для анализа больших данных телеметрии с целью проактивного выявления аномалий и кибератак, а также для автоматизации реагирования на инциденты (SOAR).

Безопасность Интернета Вещей (IoT): разработка стандартов и решений для защиты миллиардов "умных" устройств, от камер до промышленных контроллеров, которые часто имеют слабую встроенную защиту.

Квантовая криптография: создание систем шифрования, устойчивых к взлому даже квантовыми компьютерами, что является ответом на будущие вызовы.

Концепция «нулевого доверия» (Zero Trust): отход от модели «замок и ров» (защищенный периметр) к подходу «никому не доверяй, проверяй всегда». Каждый

запрос к ресурсу проверяется, независимо от его источника.

Управление цифровыми идентификаторами и доступом (IAM): развитие биометрических и поведенческих методов аутентификации, систем одноразовых паролей для обеспечения надежного контроля доступа.

Повышение осведомленности и обучение: борьба с «человеческим фактором» через непрерывное и иммерсивное обучение сотрудников, включая кибертренажеры и симуляции фишинговых атак.

7. Необходимость обеспечения информационной безопасности.

Необходимость обеспечения ИБ продиктована фундаментальными потребностями современного цифрового общества. Без нее становится невозможным:

Защита национального суверенитета: информационные атаки могут дестабилизировать политическую ситуацию, повлиять на избирательные процессы, подорвать обороноспособность.

Стабильное экономическое развитие: киберпреступность наносит многомиллиардные убытки бизнесу, кража интеллектуальной собственности подрывает конкурентоспособность.

Сохранение прав и свобод граждан: утечки персональных данных, тотальная слежка, цифровое мошенничество напрямую нарушают право на частную жизнь и конфиденциальность.

Функционирование критической инфраструктуры: работа энергосистем, транспорта, здравоохранения, финансов сегодня полностью зависит от информационных систем, выход которых из строя грозит катастрофой. Таким образом, ИБ — это не роскошь, а обязательное условие существования и развития государства, бизнеса и личности в XXI веке.

8. Основные понятия информационной безопасности.

Для понимания предмета необходимо оперировать базовыми понятиями:

Информационная безопасность: состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Угроза (информационной безопасности): совокупность условий и факторов, создающих опасность для жизненно важных интересов личности, общества и государства в информационной сфере.

Уязвимость (уязвимое место): слабость в системе, процедуре или контроле, которая может быть использована злоумышленником для реализации угрозы.

Атака (кибератака): целенаправленное действие злоумышленника по реализации угрозы, использующее уязвимости информационной системы.

Инцидент (информационной безопасности): любое нежелательное событие, которое привело или может привести к нарушению конфиденциальности, целостности или доступности информации.

Защищаемая информация: информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации.

9. Структура понятия информационная безопасность.

Структурно понятие «информационная безопасность» можно раскрыть через три уровня защищаемых интересов, как это определено в Доктрине ИБ РФ:

1. **Интересы личности:** обеспечение конституционных прав и свобод человека и гражданина, включая право на неприкосновенность частной жизни, свободу получения и распространения информации, защиту персональных данных.
2. **Интересы общества:** защита общественного согласия, духовно-нравственных ценностей, демократических институтов, стабильности и развития гражданского общества.
3. **Интересы государства:** создание условий для бесконфликтного развития страны, защиты конституционного строя, суверенитета и территориальной целостности, укрепления обороноспособности, развития цифровой экономики и обеспечения национальных интересов.

Эти три уровня взаимосвязаны и образуют единую систему, где нарушение безопасности на одном уровне неизбежно затрагивает другие.

10. Система защиты информации и ее структура.

Система защиты информации (СЗИ) – это совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации. Ее структура включает следующие основные элементы:

Правовое обеспечение: законы, нормативные акты, стандарты (например, ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ «О персональных данных», стандарты ФСТЭК).

Организационное обеспечение: регламенты, политики безопасности, инструкции для сотрудников, распределение ролей и ответственности (например, назначение ответственного за ИБ).

Технические (программно-аппаратные) средства: межсетевые экраны (firewalls), системы обнаружения и предотвращения вторжений (IDS/IPS), антивирусное ПО, средства шифрования, системы DLP (защита от утечек).

Программное обеспечение защиты: встроенные механизмы безопасности операционных систем, средства контроля доступа.

Эта структура является комплексной, и только слаженная работа всех ее компонентов обеспечивает эффективную защиту.

11. Экономическая информация как товар и объект безопасности.

Экономическая информация в современном мире является особым видом товара, обладающим стоимостью и потребительной стоимостью. Ее товарная природа проявляется в том, что ее можно покупать, продавать, обменивать и использовать для извлечения прибыли. Например, базы данных клиентов, ноу-хау, бизнес-планы, аналитические отчеты имеют прямую рыночную ценность. Как **объект безопасности**, экономическая информация является ключевым активом предприятия, утрата или компрометация которого ведет к прямым финансовым потерям, утрате конкурентных преимуществ, репутационному ущербу и, в конечном счете, к банкротству. Поэтому защита экономической информации от несанкционированного доступа, копирования, модичения или уничтожения приравнивается к защите материальных активов компании и является одной из главных задач ее службы безопасности.

12. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.

Профессиональная тайна – это информация, доверенная или ставшая известной лицу исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной службой, и не подлежащая разглашению. Виды профессиональных тайн:

1. Врачебная тайна (медицинская).
2. Адвокатская тайна (тайна предварительного следствия).
3. Нотариальная тайна.
4. Банковская тайна.
5. Тайна исповеди.
6. **Коммерческая тайна** также часто причисляется к этому перечню.

Объекты коммерческой тайны на предприятии – это сведения, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. К ним относятся:

1. Производственные технологии, ноу-хау, патенты.
2. Планы развития предприятия, бизнес-планы.
3. Данные о клиентах и поставщиках.
4. Финансовая информация (себестоимость, размер прибыли).
5. Структура и размер зарплат.
6. Маркетинговые стратегии и планы рекламных кампаний.

13. Персональные данные и их защита.

Персональные данные (ПДн) – это любая информация, относящаяся к прямо или

косвенно определенному или определяемому физическому лицу (субъекту ПДн). Защита ПДн в РФ регулируется прежде всего Федеральным законом № 152-ФЗ «О персональных данных». Меры по защите включают:

Правовые: jпределение целей обработки, получение согласия субъекта, разработка политики обработки ПДн.

Организационные: уазначение ответственного за обработку ПДн, разграничение прав доступа сотрудников, обучение персонала.

Технические: bспользование средств шифрования (криптографии), антивирусной защиты, систем DLP, ведение журналов учета и контроля для обеспечения неотвратимости наказания за нарушение.

Оператор ПДн (организация, обрабатывающая данные) обязан принимать все необходимые меры для защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

14. Информационные угрозы, их виды и причины возникновения.

Информационные угрозы – это потенциально возможные события или действия, которые могут привести к нарушению конфиденциальности, целостности или доступности информации. **Виды** угроз классифицируются по разным основаниям:

По природе возникновения: естественные (пожары, наводнения) и искусственные (умышленные и неумышленные).

По аспекту безопасности, на который направлена угроза: угрозы конфиденциальности (перехват, хищение), целостности (модификация, подлог), доступности (блокирование, вывод из строя).

По способу воздействия: пассивные (наблюдение за каналами связи без изменения данных) и активные (целенаправленное изменение системы или данных).

Причины возникновения угроз многослойны:

Объективные причины: техническое несовершенство систем, наличие «дыр» в ПО, стихийные бедствия.

Субъективные причины: «человеческий фактор» (ошибки, халатность, недовольство сотрудников), злой умысел (действия хакеров, инсайдеров, конкурентов).

15. Информационные угрозы для личности.

Для отдельного человека (личности) информационные угрозы представляют прямую опасность его правам, свободам, репутации и материальному благополучию. К ним относятся:

Нарушение приватности: сбор и распространение персональных данных без согласия, слежка через камеры наблюдения, отслеживание в интернете.

Кража личных данных (Identity Theft): использование персональной

информации (паспортные данные, СНИЛС) для получения кредитов, совершения преступлений.

Мошенничество и фишинг: обманные схемы с целью завладения банковскими реквизитами, паролями от учетных записей.

Кибербуллинг и троллинг: травля, оскорбления, шантаж и распространение компрометирующей информации в сети с целью нанесения психологического вреда.

Воздействие на психику и манипуляция сознанием: целенаправленное распространение дезинформации, пропаганды, вовлечение в деструктивные культы и сообщества.

16. Действия и события, нарушающие информационную безопасность.

К действиям и событиям, приводящим к нарушению ИБ, относятся:

Несанкционированный доступ: проникновение в систему или к данным с помощью подобранных паролей, использования уязвимостей, кражи носителей информации.

Утечка информации: неправомерная передача конфиденциальных данных третьим лицам (через email, мессенджеры, на флеш-накопителях).

Модификация или подлог данных: изменение информации с корыстной или иной целью (например, изменение оценок в базе данных вуза, сумм денежных переводов).

Отказ в обслуживании (DoS/DDoS-атака): создание условий, при которых легальные пользователи не могут получить доступ к системе или услуге.

Внедрение вредоносного программного обеспечения: заражение систем вирусами, червями, троянами, ransomware.

Нарушение установленных регламентов: действия сотрудников, нарушающие политики безопасности (использование слабых паролей, посещение подозрительных сайтов с рабочего компьютера).

17. Доктрина информационной безопасности России.

Доктрина информационной безопасности Российской Федерации – это стратегический планирующий документ, который представляет собой систему официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере. Она определяет **национальные интересы** в информационной сфере (защита личности, общества, государства), **основные угрозы** этим интересам и **стратегические цели и направления** по их нейтрализации. Доктрина служит основой для формирования государственной политики в области ИБ, разработки соответствующих программ и мероприятий. В ней, в частности, подчеркивается необходимость достижения технологической независимости России в сфере информационных технологий, развития отечественных средств защиты информации и противодействия использованию информационных технологий в военно-политических целях, недружественных Российской Федерации. Этот документ является фундаментальным для понимания государственного подхода к вопросам

информационной безопасности в стране.

4. ПОРЯДОК ПРОВЕДЕНИЯ И КРИТЕРИИ ОЦЕНИВАНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Порядок проведения промежуточной аттестации

Итоговый зачет проводится в присутствии преподавателя и предполагает развернутый, полный ответ на один теоретический вопрос. Вопросы составляются с учётом материала, пройденного как на лекционных занятиях, так и на практических занятиях. Время, отводимое на выполнение итоговой работы, 40 минут.

4.2. Критерии оценивания промежуточной аттестации по видам оценочных средств

Во время текущей аттестации студент может получить до 60 баллов (посещение занятий, активность во время практических/лабораторных занятий, выполнение заданий). Если студент не набрал 30 баллов за время семестра, то ему предоставляется возможность перед экзаменом предоставить выполненные работы и ответить на вопросы пропущенных занятий.

На экзамене студент может получить до 20 баллов за каждый этап экзамена (всего максимально 40 баллов).

При подведении итогов учитываются результаты текущей аттестации. Полученные за текущую аттестацию баллы суммируются с баллами, полученными за каждый этап при прохождении промежуточной аттестации:

0-49 баллов – «неудовлетворительно» (2): низкий уровень сформированности компетенций;

50-69 баллов – «удовлетворительно» (3): базовый уровень сформированности компетенций;

70-90 баллов – «хорошо» (4): средний уровень сформированности компетенций;

91-100 баллов – «отлично» (5): высокий уровень сформированности компетенций.

Особенности проведения процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья:

Итоговый экзамен (промежуточная аттестация) проводится в присутствии преподавателя и предполагает развернутый, полный ответ на теоретический вопрос, а затем работу за персональным компьютером. Вопросы составляются с учётом материала, пройденного как на лекционных занятиях, так и на практических занятиях. Время, отводимое на выполнение итоговой работы, 90 минут.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения: – в печатной форме увеличенным шрифтом, – в форме электронного документа.

Для лиц с нарушениями слуха: – в печатной форме, – в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата: – в печатной форме, – в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме);

б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа, задания зачитываются ассистентом);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, с использованием услуг ассистента, устно; используется голосовой мессенджер для записи ответа студента).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов. Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

4.3. Результаты промежуточной аттестации и уровни сформированности компетенций

Уровни сформированности компетенций определяются следующим образом:

1. Высокий уровень сформированности компетенций соответствует оценке «отлично»:

– предполагает готовность применять полученные знания в ситуациях, связанных с содержанием дисциплины;

– обучающийся способен аргументировать собственную точку зрения при постановке профессиональных задач;

– обучающийся демонстрирует способность вычленять заданный компонент проблем и задач, опираясь на самостоятельно проведенный поиск информации.

2. Средний уровень соответствует оценке «хорошо»:

– обучающийся освоил знания, связанные с содержанием дисциплины;

– обучающийся способен аргументировать собственную точку зрения при постановке профессиональных задач;

– обучающийся демонстрирует способность вычленять заданный компонент проблем и задач, хотя и может затрудняться в самостоятельном поиске информации.

3. Базовый уровень соответствует оценке «удовлетворительно»:

– обучающийся способен аргументировать собственную точку зрения при постановке профессиональных задач, но такая аргументация отличается неполнотой и может быть затруднена;

– обучающийся демонстрирует способность вычленять заданный компонент проблем и задач, но не может дать развернутое обоснование этого компонента; поиск информации проводит поверхностно.

4. Низкий уровень соответствует оценке «неудовлетворительно»; компетенции не сформированы и не проявлены.