МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)
ШКОЛА ЭКОНОМИКИ И МЕНЕДЖМЕНТА

СОГЛАСОВАНО
Руководитель ОП
_____ В.С.Хамидулин
(подпись) (ФИО)

УТВЕРЖДАЮ
Директор Департамента менеджмента и предпринимательства
_____ Е.Н.Яшина
(подпись) (И.О. Фамилия)
05 декабря 2022 г.

Цифровая безопасность в органах власти

Направление подготовки 38.03.02 Менеджмент
(Государственное и муниципальное управление)
Форма подготовки *очная*

курс *4* семестр *7*
лекции *18* час.
практические занятия *18* час.

всего часов аудиторной нагрузки *36* час.
самостоятельная работа *72* час.

контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 7 семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями образовательного стандарта, самостоятельно устанавливаемого ДВФУ, утвержденного приказом ректора от 04.04.2016 г. № 12-13-592

Рабочая программа обсуждена на заседании Департамента менеджмента и предпринимательства, протокол от 05 декабря 2022 №04.

Директор Департамента менеджмента и предпринимательства Е.Н. Яшина.

Составитель: Г.А. Черкунов

Владивосток
2022

Оборотная сторона титульного листа РПУД

I. Рабочая программа пересмотрена на заседании кафедры:

Рабочая программа обсуждена на заседании Департамента менеджмента и предпринимательства, протокол от 05 декабря 2022 №04.

1. Цели и задачи освоения дисциплины:

Данная дисциплина нацелена на формирование базового уровня знаний о принципах построения системы цифровой безопасности органов власти Российской Федерации и методах противодействия киберугрозам.

Задачами дисциплины является изучение принципов функционирования информационных систем органов власти, изучение подходов к проведению кибератак и методов противодействия угрозам информационной безопасности.

Профессиональные компетенции выпускников и индикаторы их достижения:

Тип задач	Код и наименование профессиональной компетенции (результат освоения)
информационно-аналитическая	ПК-11 владение навыками анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ПК-11 владение навыками анализа информации о функционировании системы внутреннего документооборота организации, ведения баз данных по различным показателям и формирования информационного обеспечения участников организационных проектов	Знает возможности и границы применения программного обеспечения анализа и качественного моделирования систем управления.
	Умеет владеть средствами программного обеспечения анализа и количественного моделирования систем управления.
	Владеет методами применения средств программного обеспечения анализа и количественного моделирования систем управления, навыками их оценки их эффективности.

2. Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 3 зачётные единицы (108 академических часов).

Видами учебных занятий и работы обучающегося по дисциплине могут являться:

Обозначение	Виды учебных занятий и работы обучающегося
Лек	Лекции
Пр	Практические занятия
СР	Самостоятельная работа обучающегося в период теоретического обучения

Структура дисциплины:

Форма обучения – очная.

№	Наименование раздела дисциплины	Семестр	Количество часов по видам учебных занятий и работы обучающегося						Формы промежуточной аттестации, текущего контроля успеваемости
			Лек	Лаб	Пр	ОК	СР	Контроль	
1	Информация в органах власти	7	2	0	2	0	0	0	Опрос
2	Система информационной безопасности		2		2		0		Опрос
3	Сбор информации из внешних источников		2		2		8		Практическая работа
4	Сбор информации из внутренних источников		2		2		8		Практическая работа
5	Атаки в отношении цифровых систем		2		2		8		Практическая работа
6	Законодательные аспекты привлечения к ответственности за совершение противных деяний в области информационной безопасности		2		2		10		Практическая работа
7	Минимизация рисков влияния человеческого фактора		2		2		10		Практическая работа
8	Методы физической защиты		2		2		10		Практическая работа
9	Цифровая безопасность органов власти		2		2		18		Практическая работа
	Итого:		18	0	18	0	72	0	108

Ш. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Общие принципы построения цифровых систем органов власти.

Данный раздел направлен на формирование знаний о принципах функционирования современных информационных систем органов власти.

Лекция 1. Информация в органах власти. Информация, как один из элементов функционирования органов власти. Основы построения современных цифровых систем.

Лекция 2. Система информационной безопасности. Принципы построения систем безопасности. Нормативные аспекты защиты информации в органах власти.

Раздел II. Угрозы цифровой безопасности.

Данный раздел направлен на изучение практики подготовки и проведения кибератак в отношении цифровых систем. Также часть раздела касается аспекта наступления ответственности за совершение правонарушений в области обеспечения информационной безопасности.

Лекция 3. Сбор информации из внешних источников. Практики OSINT. Получение информации из открытых источников.

Лекция 4. Сбор информации из внутренних источников. Социальная инженерия. Кража паролей. Передача файлов. Инсайдеры. Шпионаж. Государственная измена.

Лекция 5. Атаки в отношении цифровых систем. Методология получения несанкционированного доступа к информационным системам. Обход систем безопасности. Получение информации от сетевых сервисов. Перехват информации. Перенаправление портов и туннелирование. Вредоносный код. Атаки на веб-приложения. Беспроводные сети. Превышение привилегий. Переполнение буфера.

Лекция 6. Законодательные аспекты привлечения к ответственности за совершение противных деяний в области информационной безопасности.

Ответственность за нарушение правил информационной безопасности внутри организаций. Уголовная и административная ответственность.

Раздел III. Обеспечение цифровой безопасности.

Данный раздел раскрывает методы противодействия угрозам информационной безопасности.

Лекция 7. Минимизация рисков влияния человеческого фактора. Цифровая гигиена сотрудников. Нормативная поддержка цифровой безопасности. Обучение и тренировки. Защита от утечки информации.

Лекция 8. Методы физической защиты. Методы программной защиты. Брандмауэры. Системы обнаружения вторжения (IDS). Виртуальные защищенные системы (VPN).

Лекция 9. Цифровая безопасность органов власти. Подведение итогов курса.

IV. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Раздел I. Общие принципы построения цифровых систем органов власти.

Данный раздел направлен на формирование знаний о принципах функционирования современных информационных систем органов власти.

Практика 1. Информация в органах власти.
Формат практической работы: командная работа.
Цель: познакомить студентов принципами создания и интеграции информационных систем в организации.
Описание: Студенты делятся на команды по два-три человека. Каждой команде выдаётся карточка задания, в которой описывается, какую функцию выполняет их «подразделение» и требования к построению своей собственной информационной системы/базы данных. В центре системы стоит информация, составляющая информацию ограниченного доступа. После построения данных систем команды пытаются объединить свои системы выстроив между ними связи. Для каждой системы студенты описывают краткую инструкцию функционирования. Все результаты работ фиксируются в электронном виде и приносятся на следующее занятие.

Практика 2. Система информационной безопасности.
Формат практической работы: командная работа.
Цель: познакомить студентов с задачами построения системы информационной безопасности организации.
Описание: Студенты продолжают работать в командах прошлого учебного занятия. Работа производится на основании результатов предыдущего занятия. В новой объединённой цифровой системе студентам предлагается продумать систему цифровой безопасности. Для данной системы студенты описывают ограничения, протоколы действий и меры реагирования на наступление инцидентов информационной безопасности. После подготовки общего регламента преподаватель занимает роль нарушителя и используя уязвимости старается проникнуть в систему. При успешном проникновении в систему студентам необходимо внести изменения в протоколы безопасности. Все результаты работ фиксируются в электронном виде.

Раздел II. Угрозы цифровой безопасности.

Данный раздел направлен на изучение практики подготовки и проведения кибератак в отношении цифровых систем. Также часть раздела касается аспектов наступления ответственности за совершение правонарушений в области информационной безопасности.

Практика 3. Сбор информации из внешних источников.
Формат практической работы: индивидуальная работа.
Цель: познакомить студентов с приемами OSINT (кибербразведка).
Описание: Каждому студенту предлагается с использованием открытых источников сети интернет провести аналитические мероприятия в отношении объектов, которые предложит преподаватель - юридические или физические лица. Полученные результаты презентуются перед аудиторией и совместно обсуждаются.

Практика 4. Сбор информации из внутренних источников.
Формат практической работы: групповая работа с применением активного метода обучения (игрофикации).
Цель: моделирование ситуации реализации внутренней угрозы утечки данных.
Описание: Занятие представляет собой психологическую ролевую игру. В рамках данной игры действует нарратив: все студенты учебной группы представляют собой работников организации N. Произошла утечка информации, в рамках игры студентам необходимо выяснить, кто является источником утечки и какая информация была утерена.
Среди студентов выделяются следующие роли: рядовой работник, работник службы безопасности, работник – источник утечки. Распределение ролей происходит случайно, количество ролей зависит от количества игроков. Каждому игроку выдаётся роль и её краткое описание: последняя неделя работы, цели, задачи, возможные улики.
Аспект, проецирующий студентов на создание стрессовой ситуации заключается в том, что у каждого игрока в описании ролей заложена вероятность создания случайной утечки информации, но лишь один это сделал целенаправлено.

Практика 5. Атаки в отношении цифровых систем.
Формат практической работы: групповая работа.
Цель: сформировать навык идентификации типа кибератаки.

Описание: в рамках занятия преподаватель предлагает к обсуждению реальные примеры проведенных кибератак. Студентам предлагается определить вид проведенной атаки и её последствия для цифровой системы.

Практика 6. Законодательные аспекты привлечения к ответственности за совершение противных деяний в области информационной безопасности.
Формат практической работы: индивидуальная работа.
Цель: сформировать навык идентификации типа правонарушения и определения степени ответственности.
Описание: в рамках занятия преподаватель предлагает к обсуждению реальные примеры проведенных нарушений информационной безопасности. Студентам предлагается определить вид нарушения и степень ответственности на основании УК, АК и иных нормативных актов.

Раздел III. Обеспечение цифровой безопасности.

Данный раздел направлен на изучение методов противодействия угрозам информационной безопасности

Практика 7. Минимизация рисков влияния человеческого фактора.
Формат практической работы: командная работа с применением активного метода обучения (игрофикации).
Цель: моделирование ситуации противодействия атакам в отношении цифровой системы с использованием человеческого фактора.
Описание: в рамках игры учебная группа делится на четыре группы: атака, защита, владелец ИОД, получатель ИОД. Атакующие – злоумышленники, целью которых является хищение ИОД. Владелец ИОД – лицо, передающее ИОД получателю. Получатель – лицо принимающее ИОД. Защита – работник службы безопасности, целью которого является недопуск утечки ИОД. У каждого определены права и обязанности, инструменты воздействия и ограничения. Задача игры: сформировать понимание аудитории, что наиболее выигрышная стратегия – обеспечение защиты ИОД на уровне владельца и получателя ИОД за счет правил, инструкций и дополнительного контроля со стороны службы безопасности.

Практика 8. Методы физической защиты.
Формат практической работы: индивидуальная работа.
Цель: сформировать навык идентификации типа атаки, определить объект атаки, определить меры реагирования.

Описание: в рамках занятия преподаватель предлагает к обсуждению реальные примеры проведенных кибератак. Студентам предлагается определить вид атаки, определить объект атаки и предложить меры реагирования в краткосрочной и долгосрочной перспективе.

Практика 9. Итоговая работа.
Формат практической работы: командная работа.
Цель: обобщить знания, полученные в рамках прохождения курса.
Описание: итоговая работа представляет собой схематичную разработку упрощенной системы обеспечения цифровой безопасности предложенного преподавателем органа власти. Каждая команда предварительно получает описание технологических процессов информационных систем.

V. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ (*И ОНЛАЙН КУРСА ПРИ НАЛИЧИИ*)

В данном разделе приводится описание процесса самостоятельной работы обучающихся и методические рекомендации по её организации.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

1. Подготовительный;
2. Основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
3. Заключительный (оценка значимости и анализ результатов, их систематизация).

Контроль самостоятельной работы и оценка ее результатов организуются как единство двух форм:

1. самоконтроль и самооценка студента;
2. контроль и оценка со стороны преподавателей.

Основными формами самостоятельной работы обучающихся являются:

1. осмысление учебной информации, сообщаемой преподавателем;
2. изучение рекомендованной литературы;
3. консультация с преподавателем по сложным, непонятным вопросам;
4. подготовка к проведению зачета (в случае обучения в дистанционном формате либо ликвидации академической разницы);
5. выполнение практических заданий как индивидуальных, так и групповых, поиск и анализ дополнительной информации по дисциплине.

В течение семестра последовательно увеличивается объем самостоятельной работы по мере овладения обучающимися навыками самообразования, последовательно переходя от простых к более сложным заданиям. В течение семестра постоянно повышается творческий характер выполняемых работ, активно включается элементы обобщения практического опыта, усиливается самостоятельный характер обучения.

VI. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Код и наименование индикатора достижения	Оценочные средства	
			текущий контроль	промежуточная аттестация
1	Общие принципы построения цифровых систем органов власти	Знает возможности и границы применения программного обеспечения анализа и качественного моделирования систем управления.	Устный опрос	Итоговая практическая работа
			Выполнение практических заданий	Итоговая практическая работа
2	Угрозы цифровой безопасности	Умеет пользоваться средствами программного обеспечения анализа и количественного моделирования систем управления.	Устный опрос	Итоговая практическая работа
			Выполнение практических заданий	Итоговая практическая работа
3	Обеспечение цифровой безопасности	Владеет методами применения средств программного обеспечения анализа и количественного моделирования систем управления, навыками их оценки их эффективности.	Устный опрос	Итоговая практическая работа
			Выполнение практических заданий	Итоговая практическая работа

VII. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

Стратегические документы:

1. «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утв. Президентом РФ 24.07.2013 N Пр-1753) [Гарант]
2. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Кодекс]
3. Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 — 2030 годы» [Кодекс]
4. Указ Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации»
5. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации (утв. Секретарем Совета Безопасности Российской Федерации Н.П.Патрушевым 31 августа 2017 г.)
6. Распоряжение Правительства РФ от 03.06.2019 N 1189-р «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий («дорожную карту») по созданию национальной системы управления данными на 2019 — 2021 годы»
7. Указ Президента РФ от 10.10.2019 N 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»)
8. Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 06.07.2016) „Об оперативно-розыскной деятельности“
9. »Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 30.10.2018)
10. «Арбитражный процессуальный кодекс Российской Федерации» от 24.07.2002 N 95-ФЗ (ред. от 03.08.2018)
11. «Гражданский процессуальный кодекс Российской Федерации» от 14.11.2002 N 138-ФЗ (ред. от 03.08.2018)
12. «Кодекс административного судопроизводства Российской Федерации» от 08.03.2015 N 21-ФЗ (ред. от 19.07.2018)
13. ФСБ России. Стандарт СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения»

Системообразующие документы. (Данные документы тем или иным образом регулируют практически любую ситуацию, связанную с обеспечением информационной безопасности):

1. «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 N 51-ФЗ
2. «Гражданский кодекс Российской Федерации (часть вторая)» от 26.01.1996 N 14-ФЗ
3. «Гражданский кодекс Российской Федерации (часть третья)» от 26.11.2001 N 146-ФЗ
4. «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 N 230-ФЗ
5. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»
6. Указ Президента РФ от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера»

Ответственность за нарушения в области информационной безопасности:

1. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 03.10.2018)
2. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 11.10.2018)
3. Постановление Пленума Верховного Суда РФ от 25.12.2018 N 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» [Гарант]
4. Федеральный закон от 27.07.2010 N 224-ФЗ (ред. от 03.08.2018) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»
5. Указание Банка России от 11.09.2014 N 3379-У (ред. от 20.12.2017) «О перечне инсайдерской информации лиц, указанных в пунктах 1 — 4, 11 и 12 статьи 4 Федерального закона „О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации“ (Зарегистрировано в Минюсте России 15.10.2014 N 34325) [Кодекс]

Государственные и муниципальные информационные системы (ГИС и МИС) (Основным федеральным законом про государственные (ГИС) и муниципальные информационные системы (МИС) является Федеральный закон от 27.07.2006 N 149-ФЗ):

1. Федеральный закон от 02.05.2006 N 59-ФЗ (ред. от 27.11.2017) «О порядке рассмотрения обращений граждан Российской Федерации»
2. Федеральный закон от 22.12.2008 N 262-ФЗ (ред. от 28.12.2017) «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»
3. Федеральный закон от 09.02.2009 N 8-ФЗ (ред. от 28.12.2017) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»

Особенности использования информационных систем в государственных органах, в том числе обязанность публиковать перечни используемых информационных систем:

1. Приказ Управления делами Президента РФ от 03.10.2017 N 402 «Об утверждении Порядка организации работы по обеспечению доступа к информации о деятельности Управления делами Президента Российской Федерации» (Зарегистрировано в Минюсте России 31.10.2017 N 48737) [Кодекс]
2. Постановление Правительства РФ от 18.05.2009 N 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям» [Кодекс]
3. Постановление Правительства РФ от 24.11.2009 N 953 (ред. от 20.04.2017) «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» (вместе с «Требованиями к технологическим, программным и лингвистическим средствам обеспечения пользования официальным сайтом Правительства Российской Федерации в сети Интернет») [Кодекс]
4. Постановление Правительства РФ от 08.09.2010 N 697 (ред. от 30.06.2018) «О единой системе межведомственного электронного взаимодействия» (вместе с «Положением о единой системе межведомственного электронного взаимодействия») [Кодекс]
5. Постановление Правительства РФ от 08.06.2011 N 451 (ред. от 25.09.2018) «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме»

(вместе с «Положением об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме»)

6. Постановление Правительства РФ от 26.06.2012 N 644 (ред. от 25.09.2018) «О федеральной государственной информационной системе учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов» (вместе с «Положением о федеральной государственной информационной системе учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов») [Кодекс]
7. Постановление Правительства РФ от 10.07.2013 N 584 (ред. от 30.06.2018) «Об использовании федеральной государственной информационной системы „Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме“ (вместе с „Правилами использования федеральной государственной информационной системы “Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме») [Кодекс]
8. Постановление Правительства РФ от 31.07.2014 N 747 «О перечне личных, семейных и домашних нужд, удовлетворение которых не влечет исполнения обязанностей, предусмотренных частями 2 — 4 статьи 10.1 Федерального закона „Об информации, информационных технологиях и о защите информации“ [Кодекс]
9. Распоряжение Правительства РФ от 29.12.2014 N 2769-р (ред. от 18.10.2018) <Об утверждении Концепции региональной информатизации> [Кодекс]
10. Постановление Правительства РФ от 06.07.2015 N 675 (ред. от 25.09.2018) „О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона “Об информации, информационных технологиях и о защите информации» (вместе с «Правилами осуществления контроля за размещением технических средств информационных систем,

используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями, государственными и муниципальными учреждениями, на территории Российской Федерации», «Правилами осуществления контроля за соблюдением требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации») [Кодекс]

11. Постановление Правительства РФ от 06.07.2015 N 676 (ред. от 11.05.2017) «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» [Кодекс]
12. Постановление Правительства РФ от 14.11.2015 N 1235 (ред. от 25.09.2018) «О федеральной государственной информационной системе координации информатизации» (вместе с «Положением о федеральной государственной информационной системе координации информатизации»)
13. Постановление Правительства РФ от 31.05.2021 N 844 «Об утверждении Правил внесения абонентом — юридическим лицом либо индивидуальным предпринимателем в федеральную государственную информационную систему „Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме“ сведений, позволяющих идентифицировать абонента — юридического лица либо индивидуального предпринимателя или их пользовательское оборудование (оконечное оборудование), и установления состава указанных сведений» [КОДЕКС]
14. Постановление Правительства РФ от 02.09.2021 N 1472 «Об определении информационных систем, включенных в инфраструктуру, обеспечивающую информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, с использованием которых осуществляется информационное взаимодействие федерального органа исполнительной власти, уполномоченного Правительством Российской Федерации на осуществление государственного кадастрового учета, государственной регистрации прав, ведение Единого государственного

реестра недвижимости и предоставление сведений, содержащихся в Едином государственном реестре недвижимости, и депозитария, осуществляющего хранение электронной закладной или обездвиженной документарной закладной, и о внесении изменения в Положение об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме»

О «Госчейн» и «Мастерчейн»:

1. Постановление Правительства РФ от 22.12.2021 N 2389 «О проведении эксперимента по регистрации граждан Российской Федерации в федеральной государственной информационной системе „Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме“ с использованием мобильного приложения» (вместе с «Положением о проведении эксперимента по регистрации граждан Российской Федерации в федеральной государственной информационной системе „Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме“ с использованием мобильного приложения»)
2. Приказ Минкомсвязи РФ от 25.08.2009 N 104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования» (Зарегистрировано в Минюсте РФ 25.09.2009 N 14874)
3. Приказ Минкомсвязи России от 31.05.2013 N 127 (ред. от 15.06.2016) «Об утверждении методических указаний по осуществлению учета информационных систем и компонентов информационно-телекоммуникационной инфраструктуры» (Зарегистрировано в Минюсте России 05.11.2013 N 30318) [Кодекс]
4. Приказ Минкомсвязи России от 27.06.2013 N 149 «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети „Интернет“ в форме

открытых данных, а также для обеспечения ее использования» (Зарегистрировано в Минюсте России 16.08.2013 N 29414) [Кодекс]
5. Приказ Минкомсвязи России от 22.08.2013 N 220 (ред. от 27.03.2014) «Об утверждении методических рекомендаций для исполнительных органов государственной власти субъектов Российской Федерации по осуществлению учета и классификации информационных систем и компонентов информационно-телекоммуникационной инфраструктуры, создаваемых и приобретаемых за счет средств бюджетов субъектов Российской Федерации, а также по составу сведений, размещаемых в системе учета информационных систем» [Кодекс]
6. Приказ Минкомсвязи России от 07.12.2015 N 514 «Об утверждении порядка внесения сведений в реестр территориального размещения технических средств информационных систем и формы акта о выявленных несоответствиях сведений, содержащихся в реестре» (Зарегистрировано в Минюсте России 19.02.2016 N 41157) [Кодекс]
7. Приказ Минкомсвязи России от 11.02.2016 N 44 «Об утверждении правил размещения информации в федеральной государственной информационной системе координации информатизации» (Зарегистрировано в Минюсте России 25.05.2016 N 42260) [Кодекс]
8. Государственные и муниципальные информационные системы. СМЭВ
9. Приказ Минкомсвязи России от 23.06.2015 N 210 (ред. от 22.02.2017) «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия» (Зарегистрировано в Минюсте России 25.08.2015 N 38668) [ГАРАНТ]

Учебная литература:

1. Ревнивых, А. В. Информационная безопасность в организациях: учебное пособие / А. В. Ревнивых. — Москва: Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт].
2. Информационная безопасность. Практические аспекты: учебник для вузов / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург: Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]
3. Фороузан, Б. А. Криптография и безопасность сетей: учебное пособие / Б. А. Фороузан; под редакцией А. Н. Берлина. — 3-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи

Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт].
4. Гребенникова, А. А. Инновационные технологии в деятельности органов власти: учебное пособие / А. А. Гребенникова, О. Г. Кирилюк. — Саратов: Вузовское образование, 2020. — 103 с. — ISBN 978-5-4487-0606-6. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]
5. Гребенникова, А. А. Инновационные технологии в деятельности органов власти: словарь-справочник / А. А. Гребенникова, О. Г. Кирилюк. — Саратов: Вузовское образование, 2019. — 78 с. — ISBN 978-5-4487-0500-7. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]
6. Боташева, Л. Э. Правовое регулирование доступа к информации о деятельности органов публичной власти: практикум / Л. Э. Боташева, М. С. Трофимов. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 98 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]
7. Ревнивых, А. В. Информационная безопасность в организациях: учебное пособие / А. В. Ревнивых. — Москва: Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт].

Дополнительная литература

Основы законодательства:

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)
2. Федеральный закон от 14.06.1994 N 5-ФЗ (ред. от 01.07.2017) «О порядке опубликования и вступления в силу федеральных конституционных законов, федеральных законов, актов палат Федерального Собрания»
3. Комментарий. Данный закон и изданные на его основе документы определяют случаи, при которых нормативно-правовые акты государственных регуляторов считаются обязательными к применению.
4. Указ Президента РФ от 23.05.1996 N 763 (ред. от 29.05.2017) «О порядке опубликования и вступления в силу актов Президента Российской Федерации, Правительства Российской Федерации и нормативных правовых актов федеральных органов исполнительной власти»
5. Постановление Правительства РФ от 13.08.1997 N 1009 (ред. от 31.10.2018) «Об утверждении Правил подготовки нормативных правовых актов

федеральных органов исполнительной власти и их государственной регистрации»

6. Приказ Минюста РФ от 04.05.2007 N 88 (ред. от 26.05.2009) «Об утверждении Разъяснений о применении Правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации» (Зарегистрировано в Минюсте РФ 14.05.2007 N 9449)
7. Положение Банка России от 22.09.2017 N 602-П «О правилах подготовки нормативных актов Банка России»

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Страницы и блоги крупных компаний, посвященные теме обеспечения цифровой безопасности:

1. Microsoft - https://www.microsoft.com/security/blog/
2. ESET - https://www.welivesecurity.com/research/
3. Palo Alto - https://unit42.paloaltonetworks.com/
4. NTT Security - https://insight-jp.nttsecurity.com/
5. Symantec - https://symantec-enterprise-blogs.security.com/blogs/
6. Recorded Future - https://www.recordedfuture.com/blog/?__cf_chl_jschl_tk__=.pAi10cVtRuB.WL.eeSZicB2Xu1HVmtmwq5HDmuha7A-1642311284-0-gaNycGzNCSU

Перечень информационных технологий и программного обеспечения

Группа программных средств «Microsoft Office» либо «Open Office».

VIII.МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Освоение студентами лекционного и практического материала включает в себя обязательное присутствие на занятиях (в случае дистанционного формата занятий – изучение материала в онлайн формате) выполнение всех заданий. Необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Практические занятия позволяют развивать у студентов творческое теоретическое мышление, умение самостоятельно изучать литературу, анализировать практику; учат четко формулировать мысль, вести дискуссию, то есть имеют исключительно важное значение в развитии самостоятельного мышления.

Студенту необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов.

Выполняя практические задания, студент можете обращаться за методической помощью к преподавателю. Обращаясь за помощью, необходимо хорошо продумать вопросы, которые требуют разъяснения.

IX. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные занятия по дисциплине проводятся в помещениях, оснащенных ПЭВМ с установленными на них программными средствами, мультимедийным оборудованием, выходом в сеть интернет.

Перечень материально-технического и программного обеспечения дисциплины приведен в таблице.

Материально-техническое и программное обеспечение дисциплины:

Наименование специальных помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**
Учебная аудитория для проведения занятий лекционного типа; учебная аудитория для проведения занятий семинарского типа (практических занятий); учебная аудитория для текущего контроля и промежуточной аттестации (от 40 посадочных мест)	Автоматизированное рабочее место преподавателя, магнитно-маркерная доска, Wi-FI Мобильное устройство ПЭВМ Экран для демонстрации изображений; Проектор; Подсистема аудиовывода и звукоусиления; стабильное подключение к сети интернет.	Группа программных средств «Microsoft Office» либо «Open Office», Браузер.

X. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Фонды оценочных средств включают в себя: перечень форм оценивания, применяемых на различных этапах формирования компетенций в ходе освоения дисциплины. Итоговая оценка складывается из полученных студентами баллов по мероприятиям промежуточного контроля и мероприятия промежуточной аттестации.

Задания текущего контроля:

№	Наименование критерия	Балл	Вид мероприятия промежуточного контроля
Задания текущего контроля			
1	Выполнение практической работы №1. Информация в органах власти	Max 7	Практическая работа
2	Выполнение практической работы №2. Система информационной безопасности	Max 7	Практическая работа
3	Выполнение практической работы №3. Сбор информации из внешних источников	Max 7	Практическая работа
4	Выполнение практической работы №4. Сбор информации из внутренних источников	Max 7	Практическая работа
5	Выполнение практической работы №5. Атаки в отношении цифровых систем	Max 7	Практическая работа
6	Выполнение практической работы №6. Законодательные аспекты привлечения к ответственности за совершение противных деяний в области информационной безопасности	Max 7	Практическая работа
7	Выполнение практической работы №7. Минимизация рисков влияния человеческого фактора	Max 7	Практическая работа
8	Выполнение практической работы №8. Методы физической защиты	Max 7	Практическая работа
Задание промежуточной аттестации			
1	Итоговая практическая работа. Цифровая безопасность органов власти	Max 44	Итоговая практическая работа
	ИТОГО	**Max 100**	

Текущая аттестация студентов по дисциплине «Цифровая безопасность органов власти» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной. Текущая аттестация проводится в

форме оценки качества выполненных практических работ, выполненных студентами, и осуществляется ведущим преподавателем. Промежуточная аттестация студентов по дисциплине «Цифровая безопасность органов власти» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Вид промежуточной аттестации – выполнение итоговой работы (зачет), включающей в себя выполнение практической работы и ответы на вопросы преподавателя.

Баллы и получение зачета в соответствии со сформированными компетенциями:

Баллы (рейтинговой оценки)	Оценка зачета/ экзамена (стандартная)	Требования к сформированным компетенциям
61-100	*зачтено*	Студент освоил материал по дисциплине, в целом справился с задачами учебного курса, успешно выполнил итоговое задание.
Менее 61	*не зачтено*	Студент не освоил значительную часть материала по дисциплине, суммарный объем успешно выполненных практических заданий низок, допускает существенные ошибки, неуверенно, с большими затруднениями отвечает на вопросы преподавателя.