МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГАОУ ВО «СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. ректора
_____ М.В. Румянцев
«07» 08 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

«Кибербезопасность в финансах»

Красноярск 2025

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Нормативная правовая основа Программы

Дополнительная профессиональная программа (программа профессиональной переподготовки) ИТ-профиля «Кибербезопасность в финансах» (далее — Программа) разработана в соответствии с нормами Федерального закона РФ от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»; постановлением Правительства РФ от 11 октября 2023 г. № 1678 «Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»; приказом Минобрнауки России от 19 октября 2020 г. № 1316 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности» (далее – приказ Минобрнауки России № 1316); методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов (утв. Минобрнауки России 22 января 2015 г. № ДЛ-1/05вн); с учетом требований приказа Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», с изменениями, внесенными приказом Минобрнауки России от 15 ноября 2013 г. № 1244 «О внесении изменений в Порядок организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденный приказом Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499»; приказа Министерства образования и науки РФ от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»; паспорта федерального проекта «Развитие кадрового потенциала ИТ-отрасли» национальной программы «Цифровая экономика Российской Федерации»; постановления Правительства Российской Федерации от 13 мая 2021 г. № 729 «О мерах по реализации программы стратегического лидерства «Приоритет-2030» (в редакции постановления Правительства Российской Федерации от 14 марта 2022 г. № 357 «О внесении изменений в постановление Правительства Российской Федерации от 13 мая 2021 г. № 729»); приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28 февраля 2022 г. № 143 «Об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика Российской Федерации» и признании утратившими силу некоторых приказов Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации об утверждении методик расчета показателей федеральных проектов национальной программы «Цифровая экономика

Российской Федерации»; федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии (уровень бакалавриата), утвержденного приказом Минобрнауки России от 19 сентября 2017 г. № 926, (далее — ФГОС ВО), а также профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты РФ от 1 сентября 2016 г. № 522н.

Профессиональная переподготовка заинтересованных лиц (далее — Слушатели), осуществляемая в соответствии с Программой, имеющей отраслевую направленность «Информационно-коммуникационные технологии», проводится в ФГАОУ ВО «Сибирский федеральный университет» (далее — Университет) в соответствии с учебным планом в очно-заочной форме обучения.

Разделы, включенные в учебный план Программы, используются для последующей разработки календарного учебного графика, учебно-тематического плана, рабочих программ модулей (дисциплин), оценочных и методических материалов. Перечисленные документы разрабатываются Университетом самостоятельно, с учетом актуальных положений законодательства об образовании, законодательства в области информационных технологий и смежных областей знаний ФГОС ВО и профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей».

1.2. Цель программы

Целью ДПП ПП является формирование у слушателей, обучающихся по ОП ВО – программам бакалавриата и программам специалитета (начиная со 2 курса), программам магистратуры (начиная с 1 курса) по специальностям и направлениям подготовки, относящимся к экономике, финансам и управлению цифровых компетенций в области применения методов и средств защиты информации для решения профессиональных задач, а также приобретение по итогам прохождения ДПП ПП новой квалификации «Специалист по безопасности компьютерных систем и сетей».

1.3. Требования к поступающим

К обучению по Программе допускаются обучающиеся по ОП ВО – программам бакалавриата и программам специалитета (начиная со 2 курса), программам магистратуры (начиная с 1 курса) по специальностям и направлениям подготовки, относящимся к экономике, финансам и управлению.

1.4. Характеристика новой квалификации и связанных с ней видов профессиональной деятельности, трудовых функций и(или) уровней квалификации

1.4.1. Область профессиональной деятельности слушателя, прошедшего обучение по программе профессиональной переподготовки, в которой может осуществлять профессиональную деятельность: Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере).

Выпускники могут осуществлять профессиональную деятельность в других областях и(или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

1.4.2. Объекты профессиональной деятельности: объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, информационные ресурсы и информационные технологии в условиях существования угроз в информационной сфере; технологии обеспечения информационной безопасности объектов различного уровня (система, объект системы, компонент объекта), которые связаны с информационными технологиями, используемыми на этих объектах; процессы управления информационной безопасностью защищаемых объектов.

Виды профессиональной деятельности: защита информации в компьютерных системах и сетях.

1.4.3. Уровень квалификации. В соответствии с приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 522н «Об утверждении Профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», дополнительная профессиональная программа профессиональной переподготовки «Кибербезопасность в финансах» обеспечивает достижение шестого уровня квалификации.

1.4.4. Компетенции (трудовые функции) в соответствии с профессиональным стандартом (формирование новых или совершенствование имеющихся)

Программа разработана в соответствии с актуальными квалификационными требованиями, профессиональными стандартами специалистов. Виды профессиональной деятельности, трудовые функции, указанные в профессиональном стандарте 06.032 «Специалист по безопасности компьютерных систем и сетей», представлены в таблицах 1–2.

Таблица 1

Характеристика новой квалификации, связанной с видом профессиональной деятельности и трудовыми функциями в соответствии с профессиональным стандартом 06.032 «Специалист по безопасности компьютерных систем и сетей»

Трудовые действия	Трудовая функция	Обобщенная трудовая функция	Вид профессиональной деятельности
Установка программно-аппаратных средств защиты информации	A/01.5 Техническое обслуживание программно-аппаратных средств защиты информации в операционных системах	A Техническое обслуживание средств защиты информации в компьютерных системах и сетях	Защита информации в компьютерных системах и сетях
Установка средств антивирусной защиты в соответствии с действующими требованиями			
Установка программно-аппаратных средств защиты информации в компьютерных сетях	A/02.5 Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях		
Настройка программно-аппаратных средств защиты информации в компьютерных сетях по заданным шаблонам			
Настройка программного обеспечения с соблюдением требований по защите информации	A/03.5 Техническое обслуживание средств защиты информации прикладного и системного программного обеспечения		
Определение состава применяемых программно-аппаратных средств защиты информации в операционных системах	B/01.6 Администрирование подсистем защиты информации в операционных системах	B Администрирование средств защиты информации в компьютерных системах и сетях	
Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях	B/02.6 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях		

Таблица 2

Характеристика новой и развиваемой цифровой компетенции в ИТ-сфере, связанной с уровнем формирования и развития в результате освоения программы «Кибербезопасность в финансах»

Наименование сферы	**Тип компетенции**	**Наименование компетенции**	**Номер компетенции (ID)**	**БАЗОВЫЙ УРОВЕНЬ РАЗВИТИЯ КОМПЕТЕНЦИЙ**
Прикладные программные комплексы и системы	Компетенция применима в различных отраслях экономики	Дорабатывает конфигурации и модули ИС (информационные системы) предприятий	21	Участвует в проектах доработки ИС предприятий в составе проектной команды под контролем
Информационная безопасность	Компетенция применима в различных отраслях экономики	Применяет принципы информационной безопасности (ИБ)	42	Участвует в проектах по ИБ в составе команды под контролем опытных специалистов

Таблица 3

Структура образовательных результатов

ID и формулировка целевого уровня формирования компетенций	**Промежуточные образовательные результаты**		
	Опыт практической деятельности (ОПД)	**Умения (У)**	**Знания (З)**
21. Дорабатывает конфигурации и модули ИС (информационные системы) предприятий	Анализа угроз информационной безопасности (ИБ) в финансах Разработки и внедрения мер защиты информации на объектах. Проведения аудита безопасности информационных систем. Реагирования на инциденты (работа с киберинцидентами, расследование нарушений).	Применять нормативные требования (ФЗ-187, ФЗ-152, стандарты ГОСТ Р, МЭК 62443). Настраивать защиту сетей. Использовать криптографические методы защиты данных (шифрование, ЭП).	Основы кибербезопасности (угрозы, уязвимости, атаки). Нормативно-правовую базу в области ИБ (регулирование финансовых организаций, требования ФСТЭК, ФСБ). Современные технологии защиты (IDS/IPS, honeypots, анти-DDoS).
43. Применяет принципы информационной безопасности (ИБ)	Настройка и администрирование защитного ПО (межсетевые экраны, системы обнаружения и предотвращения вторжений, антивирусные решения) Работа с криптографическими средствами (использование средств шифрования, применение электронной подписи) Мониторинг и анализ угроз	Выбирать и настраивать ПО для защиты финансовой информации. Разграничивать доступ с помощью DLP-систем. Настраивать аутентификацию	Принципы работы межсетевых экранов, IDS/IPS, антивирусов. Нормативные требования к ПО (ФСТЭК, ФСБ, ГОСТ Р 59522-2021). Методы противодействия целевым атакам.

1.5. Требования к материально-техническому обеспечению, необходимому для реализации дополнительной профессиональной программы профессиональной переподготовки (требования к аудитории, компьютерному классу, программному обеспечению)

Обучение производится на платформе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru/). Используются сервисы вебинаров и видеоконференций.

При проведении лекций, практических занятий, самостоятельной работы слушателей и практики используется следующее оборудование: компьютер с наушниками или аудиоколонками, микрофоном и веб-камерой, высокоскоростное подключение к Интернет (не менее 5 Мбит/с).

Программное обеспечение (обновленное до последней версии): браузер Яндекс, текстовый редактор.

1.6. Особенности (принципы) построения дополнительной профессиональной программы профессиональной переподготовки

Особенности построения программы переподготовки «Кибербезопасность в финансах»:

- в основу проектирования программы положен компетентностный подход;
- выполнение учебных заданий, требующих практического применения знаний и умений, полученных в ходе изучения логически связанных дисциплин;
- выполнение итоговых аттестационных работ по реальному заданию;
- использование информационных и коммуникационных технологий, в том числе современных систем технологической поддержки процесса обучения, обеспечивающих комфортные условия для обучающихся, преподавателей;
- применение электронных образовательных ресурсов (дистанционное, электронное, комбинированное обучение и пр.).

В поддержку дополнительной профессиональной программы профессиональной переподготовки разработан электронный курс на платформе http://e.sfu-kras.ru.

1.7. Особенности организации практики

Практика слушателей дополнительной профессиональной программы переподготовки «Кибербезопасность в финансах» является обязательной составной частью образовательной программы и представляет собой вид учебной деятельности, непосредственно ориентированный на профессионально-практическую подготовку слушателей. Практика осуществляется в целях формирования и закрепления профессиональных умений и навыков, полученных в результате теоретической подготовки.

Сроки проведения практики устанавливаются графиком учебного процесса в объеме 16 часов в конце процесса обучения в соответствии с утвержденным в установленном порядке учебно-тематическим планом.

В рамках очно-заочной формы обучения на основе дистанционных технологий практика осуществляется в форме online практики (в формате разработки проекта).

1.8. Документ об образовании: диплом о переподготовке установленного образца.

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы профессиональной переподготовки
«Кибербезопасность в финансах»

Форма обучения – очно-заочная.
Срок обучения – 256 часов.

№ п/п	Наименование дисциплин	Общая трудоем-кость, ч	Всего контактн., ч	Контактные часы			СРС, ч	Формы контроля
				Лекции	Лабора-торные работы	Практические и семинарские занятия		
1.	Основы цифровой безопасности	96	48	12		36	48	Зачет
2.	Защита персональных данных и безопасность цифрового следа	60	30	10		20	30	Зачет
3.	Методы и принципы безопасной работы в сети интернет	60	30	10		20	30	Зачет
6.	Практика	16	12	–		12	4	Зачет
7.	Итоговая аттестация	24	8	–		8	16	Защита итоговой аттестационной работы (проекта)
	Итого	**256**	**128**	**32**		**96**	**128**	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
дополнительной профессиональной программы профессиональной переподготовки
«Кибербезопасность в финансах»

Категория слушателей: лица, имеющие или получающие высшее образование.
Срок обучения: 256 часов.
Форма обучения: очно-заочная.
Режим занятий: 8 часов в неделю.

№ п/п	Наименование дисциплин	Общая трудоем-кость, ч	Всего контактн., ч	Контактные часы			СРС, ч
				Лекции	Лабора-торные работы	Практ. и семинарские занятия	
1	**Основы цифровой безопасности**	**96**	**48**	**12**		**36**	**48**
1.1	Методологические подходы к цифровой безопасности	16	8	2		6	8
1.2	Нормативно-правовое регулирование деятельности в области цифровой безопасности	16	8	2		6	8
1.3	Основные механизмы цифровой безопасности	16	8	2		6	8
2	**Защита персональных данных и безопасность цифрового следа**	**60**	**30**	**10**		**20**	**30**
2.1	Понятие и виды персональных данных	16	8	2		6	8
2.2	Правовой режим персональных данных. Обработка персональных данных	16	8	2		6	8
2.3	Безопасность персональных данных	16	8	2		6	8
3	**Методы и принципы безопасной работы в сети интернет**	**60**	**30**	**10**		**20**	**30**
3.1	Теоретические основы и принципы безопасной работы в сети интернет	16	8	1		6	8
3.2	Каналы утечки информации	16	8	1		6	8
3.3	Методы и средства защиты информации в сети интернет	16	8	2		6	8
4	Практика	16	12			12	4
	Итоговая аттестация	**24**	**8**	**-**		**8**	**16**
	Всего	**256**	**128**	**32**		**96**	**128**

Календарный учебный график
дополнительной профессиональной программы профессиональной переподготовки
«Кибербезопасность в финансах»

Наименование модулей (курсов) Объем учебной нагрузки, ч.	2025–2026 учебный год																																											
	сентябрь					октябрь					ноябрь				декабрь				январь				февраль				март				апрель				май					июнь				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
Основы цифровой безопасности																																												
Защита персональных данных и безопасность цифрового следа																																												
Методы и принципы безопасной работы в сети интернет																																												
Практика																																												
Итоговая аттестация																																												

II. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Обучение по программе профессиональной переподготовки «Кибербезопасность в финансах» реализовано в формате смешанного обучения, с применением активных технологий совместного обучения в электронной среде (синхронные и асинхронные занятия). Лекционный материал представляется в виде комплекса мини-видеолекций, записей занятий, текстовых материалов, презентаций, размещаемых в системе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru). Данные материалы сопровождаются заданиями и дискуссиями в чате программы. Изучение теоретического материала (СРС) предполагается до и после синхронной части работы.

Материально-технические условия реализации дисциплины

Синхронные занятия реализуются на базе инструментов видеоконференцсвязи и включают в себя практические занятия, сочетающие в себе ответы на вопросы, связанные с материалом лекции, в формате дискуссий, а также групповую и индивидуальную работу. Для проведения синхронных занятий (вебинаров со спикерами) применяется программа видеоконференцсвязи SaluteJazz.

Учебно-методическое и информационное обеспечение дисциплины

Программа может быть реализована как очно, так и заочно, в том числе с применением дистанционных образовательных технологий. Она включает занятия лекционного типа, семинарские, активные и ситуативные методы обучения.

По программе разработан электронный учебно-методический комплекс (УМК) — электронный курс в системе электронного обучения СФУ «е-Курсы». Обучающиеся могут дополнить представленные материалы, подключая к учебной работе иные источники информации, освещающие обсуждаемые проблемы.

Содержание комплекта учебно-методических материалов

Учебно-методический комплекс содержит: систему навигации по программе (учебно-тематический план, интерактивный график работы по программе, сведения о результатах обучения, о преподавателе дисциплины, чат для объявлений и вопросов преподавателю), набор презентации к лекциям, набор ссылок на внешние образовательные ресурсы и инструменты, систему заданий с подробными инструкциями, списки основной и дополнительной литературы. В электронном курсе реализована система обратной связи, а также онлайн-площадки для взаимного обучения.

Виды и содержание самостоятельной работы

Выполнение самостоятельной работы слушателями предполагается в дистанционном режиме в рамках электронного курса, размещенного в системе электронного обучения СФУ. Самостоятельно слушателями изучаются представленные кейсы с лучшими практиками, дополнительные ссылки и материалы по темам курса, а также краткие резюмирующие материалы,

дополнительные инструкции в различных форматах (видео, скринкасты, подкасты, интерактивные справочники, текстовые пояснения).

Также слушатели самостоятельно проводят анализ и систематизацию материала в рамках выполнения практических заданий и решения ситуаций. Для оценки уровня усвоения изученного учебного материала, слушатели проходят контрольные тесты.

III. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

3.1. Учебно-методическое обеспечение, в т.ч. электронные ресурсы сети Интернет

Модуль 1. Основы информационной безопасности

1. Защита информации: учеб. пособие / А.П. Жук [и др.]. – 2-е изд. – М.: ИЦ РИОР; М.: НИЦ ИНФРА-М, 2015. – 392 с. (доступ из электронной библиотеки).

2. Информационная безопасность и защита информации: учебник / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. – М.: РИОР, 2013. – 222 с. (доступ из электронной библиотеки).

3. Информационная безопасность предприятия: учеб. пособие / Н.В. Гришина. – 2-е изд. доп. – М.: Форум; М.: НИЦ ИНФРА-М, 2015. – 240 с. (доступ из электронной библиотеки).

Модуль 2. Защита персональных данных и безопасность цифрового следа

1 Управление информационной безопасностью: учебное пособие для высшего профессионального образования / В.Т. Еременко, М.Ю. Рытов, П.Н. Рязанцев, М.Н. Орешина. – Орел: ФГБОУ ВПО «Госуниверситет - УНПК», 2015. – 265 с.

2 Основы управления информационной безопасностью / Курило Л.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. – Учебное пособие для ВАЗ-ов, - М:Горячая линия Телеком, 2013, - 244 с.

3 Репин В.В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов. — М.: РИА «Стандарты и качество», 2008, 408 с.

4 ГОСТ Р ИСО/МЭК 27000-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. - Москва, Стандартинформ 2021, - 28 с.

5 ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. - Москва, Российский институт стандартизации 2021, - 29 с.

6 ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. - Москва, Российский институт стандартизации 2021, - 74 с.

7 ГОСТ Р ИСО/МЭК 27003-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. – Москва, Стандартинформ 2021 – 38 с.

8 ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Москва: Стандартинформ, 2011 – 51 с.

9 ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. – Москва: Стандартинформ, 2016 – 26 с.

10 ГОСТ Р ИСО/МЭК 27034-1-2014 Информационная технологи. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия. – Москва: Стандартинформ, 2015 – 81 с.

Модуль 3. Методы и принципы безопасной работы в сети интернет

1. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. – М.: ГЛТ, 2016. – 586 с.
2. Емельянова, Н.З. Защита информации в персональном компьютере: учеб. пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – М.: Форум, 2013. – 368 с.
3. Жук А.П. Защита информации: учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. – 392 с.
4. Ищейнов В.Я. Защита конфиденциальной информации: учеб. пособие / В.Я. Ищейнов, М.В. Мецатунян. – М.: Форум, 2013. – 256 с.
5. Малюк А.А. Защита информации в информационном обществе: учеб. пособие для вузов / А.А. Малюк. – М.: ГЛТ, 2015. – 230 с.
6. Платонов В.В. Программно-аппаратные средства защиты информации вычислительных сетей: учеб. пособие: допущено УМО. – М.: Академия, 2007. – 240 с.
7. Хорев П.Б. Программно-аппаратная защита информации: учеб. пособие / П.Б. Хорев. – М.: Форум, 2013. – 352 с.
8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.
9. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – М.: ДМК Пресс, 2017. – 702 с.
10. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ, НИЦ ИНФРА–М, 2013. – 592 с.

IV. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4.1. Формы аттестации, оценочные материалы, методические материалы

Программа предусматривает проведение текущей и итоговой аттестации. Текущая аттестация слушателей проводится по дисциплинам на основе выполнения заданий в электронном обучающем курсе, а также с учетом результатов промежуточного ассесмента.

Методические материалы, необходимые для выполнения текущих заданий, представлены в соответствующих элементах электронного обучающего курса и включают описание задания, методические рекомендации по его выполнению, критерии оценивания.

4.2. Требования и содержание итоговой аттестации

После завершения обучения по Программе обучающиеся допускаются к итоговой аттестации. Аттестация проводится с участием представителей профильных индустриальных партнеров. Итоговая аттестация по программе включает выполнение итоговой аттестационной работы (ИАР) в форме проекта. Основная цель итоговой аттестационной работы— выполнить работу, демонстрирующую уровень подготовленности к самостоятельной профессиональной деятельности.

ИАР выполняется индивидуально или в группах по 2-4 человека. Слушатель предоставляет результат выполненной работы в формате PDF, оформленной и отвечающей требованиям к содержанию итоговой аттестационной работы. Список использованных источников литературы приводится в конце ИАР. Документ прикрепляется в организационный электронный курс программы профессиональной переподготовки. В итоговой аттестационной работе должны быть четко обозначены область и актуальность работы, постановка задачи, приведены результаты, полученные слушателем. Требования и содержание итоговой аттестации изложены в методических указания к выполнению ИАР и размещаются на платформе электронных курсов СФУ.

Выполнение итоговой аттестационной работы является обязательным.

По результатам выполнения ИАР аттестационная комиссия принимает решение о предоставлении слушателям по результатам освоения дополнительной профессиональной программы профессиональной переподготовки права заниматься профессиональной деятельностью в сфере разработки программного обеспечения и выдаче диплома о профессиональной переподготовке.

Примерные задания на выполнение ИАР.

Вариант 1: Разработка системы защиты персональных данных для микрофинансовой организации

Описание:

Анализ угроз обработки ПДн в компаниях малого бизнеса (HR, клиентские базы). Разработка и внедрение бюджетного решения на основе DLP, шифрования и политик доступа.

Компетенции, оцениваемые в задании:

1. Дорабатывает конфигурации и модули ИС (информационные системы) предприятий	
Показатели оценки	Оценка/норма
Анализ используемых средств защиты в организации	Оценка: Описание информационной инфраструктуры организации и используемых средств защиты. Норма: Описание структурировано.
Организация проекта	Оценка: проект структурирован логически и удобен для навигации. Норма: Наличие четкой структуры.
2. Применяет принципы информационной безопасности (ИБ)	
Показатели оценки	Оценка/норма
Знание 152-ФЗ	Оценка: имеется понимание основных норм закона и методов его применения. Норма: Четкое понимание закона и подзаконных актов.
Навыки настройки DLP (например, MyDLP).	Оценка: приведено описание настроек. Норма: Описание структурировано.
Обоснованность решений	Оценка: все методы обоснованы. Норма: отчет должен содержать объяснение выбора методов защиты.

Вариант 2: Анализ фишинговой атаки

Описание:

Провести расследование подозрительного email (предоставленного преподавателем):

- Определить признаки фишинга (домен отправителя, ссылки, вложения).
- Использовать инструменты (VirusTotal, Email Header Analyzer).

- Предложить меры защиты для сотрудников.

Компетенции, оцениваемые в задании:

1. Дорабатывает конфигурации и модули ИС (информационные системы) предприятий	
Показатели оценки	Оценка/норма
Использование интегрированной среды и предложение её доработки	Оценка: По результатам проекта должны быть предложены рекомендации для доработки системы. Норма: Рекомендации четко структурированы.
Организация проекта	Оценка: проект структурирован логически и удобен для навигации. Норма: Наличие четкой структуры.
2. Применяет принципы информационной безопасности (ИБ)	
Показатели оценки	Оценка/норма
Умение идентифицировать фишинговые атаки	Оценка: Рекомендации по обучению персонала. Норма: Рекомендации четко структурированы.
Навыки работы с инструментами анализа угроз	Оценка: Полный анализ всех угроз. Норма: Описание угроз и вариантов их нивелирования.
Обоснованность решений	Оценка: все выбранные методы обоснованы. Норма: в конце проекта представлен отчет о выборе моделей.

Вариант 3: Управление инцидентами утечки ПДн в финтех-компаниях

Описание:

Разработка регламента действий при утечке персональных данных на примере финтех-стартапа.

Компетенции, оцениваемые в задании:

1. Дорабатывает конфигурации и модули ИС (информационные системы) предприятий	
Показатели оценки	Оценка/норма
Проанализированы типовые сценарии утечек (кибератаки, ошибки сотрудников) в организации	Оценка: Описание информационной инфраструктуры организации и используемых средств защиты.

	Норма: Описание структурировано.
Организация проекта	Оценка: проект структурирован логически и удобен для навигации. Норма: Наличие четкой структуры.
2. Применяет принципы информационной безопасности (ИБ)	
Показатели оценки	Оценка/норма
Изучить требования ЦБ РФ и ФСТЭК к реагированию на инциденты	Оценка: имеется понимание основных норм и методов их применения. Норма: Четкое понимание требований.
Создать пошаговый алгоритм действий для компании	Оценка: проект структурирован Норма: Наличие четкой структуры.
Обоснованность решений	Оценка: все методы обоснованы. Норма: отчет должен содержать объяснение выбора методов защиты.

Эти темы могут быть адаптированы в зависимости от интересов студентов и специфики их обучения. Обучающиеся предоставляется право самостоятельно определить тему ИАР. Приветствуется выбор темы итогового проекта, связанный с профессиональной деятельностью студента по основному направлению подготовки или специальности.

Структура и содержание итоговой аттестационной работы

Задачи итоговой аттестационной работы должны иметь практическое значение. Во введении ИАР должна быть обоснована актуальность работы и сущность исследуемой проблемы, раскрыты цель, задачи, объект и предмет проектирования (разработки), методы выполнения проектирования (разработки). Как правило, ИАР состоит из 3 разделов (глав).

Глава 1 содержит обзор литературы по теме работы, в котором должны быть освещены различные точки зрения по затронутым в работе вопросам и обязательно сформулировано авторское отношение к ним, характеристика объекта и предмета исследования.

Глава 2 содержит характеристику методов выполнения работы, а также техническое задание на разработку.

Глава 3 содержит характеристику результатов выполнения работы и их интерпретацию.

В заключении формулируются конкретные выводы по работе и предложения по их реализации.

Этапы выполнения ИАР задаются графиком выполнения и контролируются руководителем. Примерный список основных этапов выполнения проекта представлен ниже:

1. Выбор темы ИАР. В начале обучения за студентом закрепляется руководитель итоговой работы, который прорабатывает тему. При выборе темы итогового проекта берется во внимание вопросы, связанные с профессиональной деятельностью студента по основному направлению подготовки или специальности.
2. Формулировка цели и задач ИАР работы. Обоснование актуальности выбранного направления работы.
3. Поиск аналогичных решений, формирование концепции предлагаемых подходов, методов.
4. Выбор и/или проектирование программного, технического и иных видов обеспечений для достижения цели и решения задач ИАР.
5. Реализация проекта.
6. Формирование итоговой аттестационной работы.
7. Представление ИАР аттестационной комиссии.

Критерии оценивания итоговой аттестационной работы

Оценка	Критерии
«Отлично»	− ИАР структурирована, полностью раскрывает тему и аргументирует её актуальность; − в ИАР чётко обозначены цель и задачи; − обучающийся подчёркивает наиболее значимые выводы о проделанной работе; − обучающийся к показывает перспективы и задачи дальнейшего исследования данной темы; − обучающийся использует современные информационные технологии
«Хорошо»	− ИАР содержит описание целей и задач, но допускаются неточности при их раскрытии; − заключения и выводы недостаточно чётко сформулированы
«Удовлетворительно»	− ИАР содержит описание целей и задач, но некоторые из них не достигнуты; − обучающимся допускаются грубые нарушения в логике формулирования выводов; − обучающийся слабо подкрепляет выводы положениями из нормативно-правовых актов, выводами и расчётами
«Неудовлетворительно»	− ИАР не структурирована; − очень слабо раскрыта актуальности темы; − не определены цели и задачи; − обучающийся допускает грубые логические нарушения в определении выводов; − обучающийся не подкрепляет свои выводы положениями из нормативно – правовых актов и расчётами

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)
«Основы информационной безопасности»

1. Аннотация

Дисциплина «Основы информационной безопасности» предназначена для изучения принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации на предприятии, освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты.

Цель модуля (результаты обучения)

Модуль направлен на формирование у слушателей базовых знаний и практических навыков в области защиты информации в корпоративной среде. Основные цели:

1. Теоретические цели
   - Сформировать понимание ключевых принципов ИБ:
     - Конфиденциальность, целостность, доступность (CIA-триада).
     - Управление рисками (идентификация, оценка, минимизация угроз).
   - Изучить нормативно-правовую базу:
     - Основные законы (ФЗ-152 «О персональных данных», ФЗ-187 «О безопасности КИИ», 149-ФЗ «Об информации»).
     - Стандарты и регуляторы (ГОСТ Р 57580, ISO 27001, требования ФСТЭК, ФСБ).
   - Разобрать угрозы и уязвимости:
     - Виды кибератак (фишинг, DDoS, APT, ransomware).
     - Утечки данных и инсайдерские угрозы.
2. Практические цели
   - Научить применять базовые меры защиты:
     - Разграничение прав доступа (ролевая модель, принцип минимальных привилегий).
     - Резервное копирование и восстановление данных.
   - Отработать навыки работы с защитным ПО:
     - Настройка антивирусов, межсетевых экранов.
     - Использование DLP-систем для предотвращения утечек.
   - Познакомить с инцидент-менеджментом:
     - Алгоритм реагирования на утечки данных и кибератаки.
     - Документирование инцидентов.
3. Организационные цели
   - Развить культуру ИБ среди сотрудников:
     - Проведение инструктажей и обучение по цифровой гигиене.
     - Противодействие социальной инженерии.
   - Сформировать основы политик безопасности:

- Разработка регламентов (Политика ИБ, инструкции по работе с данными).
- Аудит и мониторинг соблюдения требований.

2. Содержание

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Модуль 1. Основы цифровой безопасности (96 часов)			
1.1. Методологические подходы к цифровой безопасности (32 ч.)	Основные понятия и термины. Политика информационной безопасности. Стратегия национальной безопасности РФ. Понятие модели нарушителя информационной безопасности. Принципы, средства и методы аутентификации. Доступность, целостность, конфиденциальность. Угрозы информационной безопасности (4 ч.)	Моделирование угроз информационной безопасности (12 ч.) *Задание 1*. Определение актуальных угроз безопасности в информационной системе	Изучение политик информационной безопасности. Тестирование (16 ч.)
1.2. Нормативно-правовое регулирование деятельности в области цифровой безопасности (32 ч.)	Федеральные законы по защите информации. Понятие и виды защищаемой информации. Юридическая ответственность в области информационной безопасности. Лицензирование сертификация и аттестация в области защиты информации. Группа стандартов 27000. Группа стандартов «Общие критерии» (4 ч.)	Нормативно-правовые акты в области информационной безопасности (12 ч.). *Задание 2.* Подготовка презентаций по стандартам в области информационной безопасности	Изучение законодательства РФ в области защиты информации. Тестирование (16 ч.)
1.3. Основные механизмы цифровой безопасности (32 ч.)	Идентификация. Аутентификация (принципы, виды). Авторизация. Контроль доступа (системы разграничения доступа). Технологии резервирования данных (в том числе RAID). Регистрация событий безопасности. Типы событий. Гарантированное затирание данных (механизм проверки). Обеспечение целостности.	Изучение средств защиты информации от несанкционированн ого доступа (12 ч.). *Задание 3.* Настройка элементов политики безопасности с помощью одного из средств защиты информации	Изучение штатных средств операционной системы. Тестирование (16 ч.)

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
	Контроль доступа к устройствам. Сигнализация попыток нарушения защиты. Восстановление средств защиты информации Компьютерные вирусы. Принципы и методы защиты от разрушающих программных воздействий. Виды атак на информационные системы (атаки типа переполнение буфера, стека и кучи, атаки, основанные на изменении входных данных, атаки на web-приложения, атаки типа «отказ в обслуживании»). Требования ФСТЭК России к программному обеспечению средств защиты (4 ч.)		

3. Условия реализации программы дисциплины

Организационно-педагогические условия реализации программы

Обучение по программе реализовано в формате смешанного обучения, с применением активных технологий совместного обучения в электронной среде (синхронные и асинхронные занятия). Лекционный материал представляется в виде синхронных лекций, записей занятий, текстовых материалов, презентаций, размещаемых в электронном курсе. Данные материалы сопровождаются заданиями и дискуссиями в чатах дисциплин. Изучение теоретического материала (СРС) предполагается до и после синхронной части работы.

Материально-технические условия реализации программы

Синхронные занятия реализуются на базе инструментов видеоконференцсвязи и включают в себя лекционные и практические занятия. Для проведения синхронных занятий (вебинаров со спикерами) применяется программа видеоконференцсвязи. При проведении лекций, практических занятий, самостоятельной работы слушателей используется следующее оборудование: компьютер с наушниками или аудиоколонками, микрофоном и веб-камерой. Программное обеспечение (обновленное до последней версии): браузер Google Chrome, текстовый редактор. На виртуальных серверах установлено программное обеспечение Inspire, на базе ПК ViPNet,

криптопровайдер ViPNet CSP, к которому имеет доступ слушатель через браузер.

Учебно-методическое и информационное обеспечение программы

Дисциплина может быть реализована как очно, так и заочно, в том числе, с применением дистанционных образовательных технологий. Она включает занятия лекционного типа, интерактивные формы обучения, практические занятия.

Содержание комплекта учебно-методических материалов

По данной дисциплине имеется электронный учебно-методический комплекс (УМК) в системе электронных курсов СФУ. УМК содержит: систему навигации по дисциплине (учебно-тематический план, интерактивный график работы по дисциплине, сведения о результатах обучения, чат для объявлений и вопросов преподавателю), текстовые материалы к лекциям, практические и тестовые задания, списки основной и дополнительной литературы. В электронном курсе реализована система обратной связи.

Литература

Основная литература

1. Защита информации: учеб. пособие / А.П. Жук [и др.]. – 2-е изд. – М.: ИЦ РИОР; М.: НИЦ ИНФРА-М, 2015. – 392 с. (доступ из электронной библиотеки).

2. Информационная безопасность и защита информации: учебник / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. – М.: РИОР, 2013. – 222 с. (доступ из электронной библиотеки).

3. Информационная безопасность предприятия: учеб. пособие / Н.В. Гришина. – 2-е изд. доп. – М.: Форум; М.: НИЦ ИНФРА-М, 2015. – 240 с. (доступ из электронной библиотеки).

Дополнительная литература

1. «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. ГОСТ Р 51188-98» (прин. Постановлением Госстандарта РФ от 14.07.1998 № 295). – М.: Стандартинформ, 1998.

2. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. ГОСТ Р 51275-2006» (утв. Приказом Ростехрегулирования от 27.12.2006 № 374-ст). – М.: Стандартинформ, 2007.

3. «Защита информации. Основные термины и определения. ГОСТ Р 50922-2006» (утв. Приказом Ростехрегулирования от 27.12.2006 № 373-ст). – М.: Стандартинформ, 2008.

4. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. ГОСТ Р.34.10-2018»

5. «Техническая защита информации. Основные термины и определения. Р 50.1.056-2005», (утв. приказом Ростехрегулирования от 29.12.2005 № 479-ст). – М.: Стандартинформ, 2006.

6. Доктрина информационной безопасности РФ, утверждена указом Президентом РФ 05.12.2016 № 646.

7. Конституция Российской Федерации.

8. Методика оценки угроз безопасности информации. Утверждена ФСТЭК России 05.02.2021.

9. Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

10. Руководящий документ. Автоматизированные системы защиты информации от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден Председателем Гостехкомиссии России, 1992.

11. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя государственной технической комиссии при Президенте Российской Федерации от 30.03.1992.

12. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД и АС и СВТ. Утвержден Гостехкомиссией России, 1992.

13. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утвержден Председателем Гостехкомиссии России, 1992.

14. Руководящий документ. Защита от НСД. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия несанкционированных возможностей. Приказ председателя Гостехкомиссии России от 04.06.1999 № 114.

15. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Утвержден Председателем Гостехкомиссии России, 1992.

16. Руководящий документ. СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации. Решение Председателя Гостехкомиссии России от 25.07.1997

17. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден Председателем Гостехкомиссии России, 1992.

18. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

19. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

20. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

21. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

22. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. Официальный сайт ФСТЭК России [Электронный ресурс]. – Режим доступа: http://www.fstec.ru.
2. Электронный каталог научной библиотеки СФУ [Электронный ресурс]. – Режим доступа: http://lib.sfu-kras.ru.

4. Оценка качества освоения программы дисциплины (формы аттестации, оценочные и методические материалы)

Форма аттестации по дисциплине — зачет.

Оценка результатов обучения осуществляется следующим образом. Максимально за курс можно набрать 100%, из них:

- тесты самоконтроля к лекциям 40 %;
- практические задания составляют 60 %.

Зачет получают слушатели, набравшие не менее 50 % из 100 от общего прогресса по курсу.

Примеры тестов для контроля знаний

1. Источником угрозы является …
   а) отсутствие или слабость защитных мер;
   б) свободный доступ к информации;
   в) то, что дает возможность использования уязвимости;
   г) риск.
2. К ключевым вопросам информационной безопасности относятся следующие вопросы:
   а) зачем надо защищаться?
   б) как и чем защищать?
   в) что следует защищать?
   г) от кого надо защищаться?
3. Субъектами информационных отношений могут быть:
   а) государство;
   б) юридические лица;
   в) физические лица;
   г) потребители.

Типовое практическое задание
Тема «Методологические подходы к защите информации и принципы ее организации»

1. Изучить методику определения актуальных угроз.
2. Определить уровень исходной защищенности ИСПДн.
3. Определить перечень актуальных угроз.

Заполнить таблицы:

Таблица 1 – Определение уровня исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4.По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+
ИСПДн с открытым доступом	–	–	+
5. *По наличию соединений с другими базами ПДн иных ИСПДн:*			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–

ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации	+	–	–
Итого			

1. ИСПДн имеет **высокий** уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий», а остальные – среднему уровню защищенности.
2. ИСПДн имеет **средний** уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний», а остальные – низкому уровню защищенности.
3. ИСПДн имеет **низкую степень исходной защищенности, если не выполняются условия по пункт**ам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

$$Y_1 =$$

Таблица 2 – Определение перечня актуальных угроз

Угроза	Y_1	Y_2	Y	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
Угрозы утечки ПДн по техническим каналам						
Утечка информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН)						
Утечка акустической (речевой) информации						
Утечка видовой информации						
Угрозы НСД к ПДн, обрабатываемым в автоматизированном рабочем месте						
Перехват паролей или идентификаторов, модификацию базовой системы ввода/вывода (BIOS) в ходе загрузки, перехват управления загрузкой						
Несанкционированное изменение ПДн						
Несанкционированное копирование ПДн						
Дефекты, сбои, аварии ТС и систем ИСПДн						
Дефекты и сбои программного обеспечения ИСПДн						
Внедрение вредоносных программ						
Обработка ПДн на незащищенных ТС обработки информации						
Копирование ПДн на незарегистрированный носитель информации						
Передача носителя информации лицу, не имеющему права доступа к ней						

Угроза	Y_1	Y_2	Y	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
Угрозы НСД к ПДн, обрабатываемых в локальных и распределенных ИСПДн						
Передача ПДн по открытым линиям связи						
Опубликование информации в открытой печати и других средствах массовой информации						
Анализ сетевого трафика с перехватом передаваемой по сети информации						
Выявление паролей						
Удаленный запуск приложений						
Внедрение по сети вредоносных программ						

1. Числовой коэффициент Y_2 вероятности возникновения угрозы определяется числом:
0 – для маловероятной угрозы;
2 – для низкой вероятности угрозы;
5 – для средней вероятности угрозы;
10 – для высокой вероятности угрозы.
2. Коэффициент реализуемости угрозы Y будет определяться соотношением:

$$Y = (Y_1 + Y_2)/20$$

3. По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:
если $0 \leq Y \leq 0{,}3$, то возможность реализации угрозы признается низкой;
если $0{,}3 < Y \leq 0{,}6$, то возможность реализации угрозы признается средней;
если $0{,}6 \leq Y \leq 0{,}8$, то возможность реализации угрозы признается высокой;
если $Y > 0{,}8$, то возможность реализации угрозы признается очень высокой.

Критерии оценивания заданий

Баллы	1 балл	2 балла	3 балла
Критерий	Задание выполнено частично, требует серьезной доработки	Задание выполнено, но требует некоторой доработки	Задание выполнено полностью, не требует доработки

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)
«Защита персональных данных и безопасность цифрового следа»

1. Аннотация

Дисциплина «Защита персональных данных и безопасность цифрового следа» предназначена для ознакомления слушателей с общими принципами построения и использования систем защиты информации, а также развитие у них навыков решения практических задач с применением современных подходов к управлению информационной безопасностью.

Цель дисциплины (результаты обучения)

Формирование у слушателей системных знаний и практических навыков по защите персональных данных (ПДн) и управлению цифровым следом в соответствии с:

- Регуляторными требованиями (152-ФЗ, отраслевые стандарты)
- Современными киберугрозами (утечки данных, фишинг, doxing)
- Технологиями защиты (анонимизация, шифрование, DLP)

2. Содержание

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Модуль 2. Защита персональных данных и безопасность цифрового следа (60 часа)			
2.1. Понятие и виды персональных данных (ПДн) (20 ч.)	ПДн понятия и виды (4 ч.)	Защита ПДн (8 ч.). *Задание 1*. План защиты ПДн	Изучение видов ПДн и создание плана защиты. Тестирование (10 ч.)
2.2. Правовой режим персональных данных. Обработка персональных данных (20 ч.)	Категории ПДн в рамках законодательства РФ (3 ч.)	Законодательные и организационные основы зашиты ПДн (6 ч.). *Задание 2.* Описание сил и средств защиты ПДн	Изучение схем построения защиты ПДн. Тестирование (10 ч.)
2.3. Безопасность персональных данных (20 ч.)	ПДн и единые требования к построению модели угроз и нарушителя (3 ч.)	Практика построения модели угроз на основе методики ФСТЭК, особенности использования БДУ фстэк (6 ч.). *Задание 3*. Исследование информационного объекта, построение плана защиты	Разработка комплекса мер защиты информации для условной организации (оператора ПДн,). Тестирование (10 ч.)

3. Условия реализации программы дисциплины

Организационно-педагогические условия реализации программы

Обучение по программе реализовано в формате смешанного обучения, с применением активных технологий совместного обучения в электронной среде (синхронные и асинхронные занятия). Лекционный материал представляется в виде синхронных лекций, записей занятий, текстовых материалов, презентаций, размещаемых в электронном курсе. Данные материалы сопровождаются заданиями и дискуссиями в чатах дисциплин. Изучение теоретического материала (СРС) предполагается до и после синхронной части работы.

Материально-технические условия реализации программы

Синхронные занятия реализуются на базе инструментов видеоконференцсвязи и включают в себя лекционные и практические занятия. Для проведения синхронных занятий (вебинаров со спикерами) применяется программа видеоконференцсвязи. При проведении лекций, практических занятий, самостоятельной работы слушателей используется следующее оборудование: компьютер с наушниками или аудиоколонками, микрофоном и веб-камерой. Программное обеспечение (обновленное до последней версии): браузер Google Chrome, текстовый редактор. На виртуальных серверах установлено программное обеспечение Inspire, на базе ПК ViPNet, криптопровайдер ViPNet CSP, к которому имеет доступ слушатель через браузер.

Учебно-методическое и информационное обеспечение программы

Дисциплина может быть реализована как очно, так и заочно, в том числе, с применением дистанционных образовательных технологий. Она включает занятия лекционного типа, интерактивные формы обучения, практические занятия.

Содержание комплекта учебно-методических материалов

По данной дисциплине имеется электронный учебно-методический комплекс (УМК) в системе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru/). УМК содержит: систему навигации по дисциплине (учебно-тематический план, интерактивный график работы по дисциплине, сведения о результатах обучения, чат для объявлений и вопросов преподавателю), текстовые материалы к лекциям, практические и тестовые задания, списки основной и дополнительной литературы. В электронном курсе реализована система обратной связи.

Литература

Основная литература

1 ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. – М.: Стандартинформ, 2016. – 26 с.

2 ГОСТ Р ИСО/МЭК 27000-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. – М.: Стандартинформ 2021. – 28 с.

3 ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Российский институт стандартизации 2021. – 29 с.

4 ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. – М.: Российский институт стандартизации 2021. – 74 с.

5 ГОСТ Р ИСО/МЭК 27003-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. – М.: Стандартинформ 2021. – 38 с.

6 ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 51 с.

7 ГОСТ Р ИСО/МЭК 27034-1-2014 Информационная технологи. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия. – М.: Стандартинформ, 2015. – 81 с.

8 Основы управления информационной безопасностью: учеб. пособие для вузов / Курило Л.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. – М.: Горячая линия Телеком, 2013. – 244 с.

9 Репин В.В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов. – М.: РИА «Стандарты и качество», 2008. – 408 с.

10 Управление информационной безопасностью: учеб. пособие для высшего профессионального образования / В.Т. Еременко, М.Ю. Рытов, П.Н. Рязанцев, М.Н. Орешина. – Орел: ФГБОУ ВПО «Госуниверситет – УНПК», 2015. – 265 с.

Перечень ресурсов информационно-телекоммуникационной сети Интернет, рекомендуемых для освоения дисциплины:

1. Подходы к организации информационной безопасности в корпоративных проектах. – URL: https://infostart.ru/1c/articles/1541897/
2. Информационная безопасность в отраслях. – URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/.
3. БДУ ФСТЭК. – URL: https://bdu.fstec.ru/threat-section.

4. Оценка качества освоения программы дисциплины (формы аттестации, оценочные и методические материалы)

Форма аттестации по дисциплине — зачет.

Оценка результатов обучения осуществляется следующим образом. Максимально за курс можно набрать 100 %, из них:

- тесты самоконтроля к лекциям 40 %;
- практические задания составляют 60 %.

Зачет получают слушатели, набравшие не менее 50 % из 100 от общего прогресса по курсу.

Примеры тестов для контроля знаний

Пример тестового задания по типу «Множественный выбор»

1. Для чего используются DCAP системы?
   a. Для автоматизированного аудита файлов и данных в ИС, поиска нарушений при обращении с конфиденциальной информацией.
   b. Для аккумулирования данных из разных сканеров безопасности и систем обнаружения атак.
   c. Для мониторинга состояния сетевого оборудования, используемого в ИС.
   d. Для сбора и анализа событий безопасности из разных источников обеспечения и контроля информационной безопасности ИС.
2. Свойство информации, которое указывает на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, называется:
   a. доступностью информации;
   b. адекватностью информации;
   c. целостностью информации;
   d. конфиденциальностью информации.
3. Потенциальная опасность для информации или системы — это:
   a. угроза;
   b. уязвимость;
   c. воздействие;
   d. риск.

Типовое практическое задание

Тема «Правовой режим персональных данных. Обработка персональных данных»

1. Составить отчёт об обследовании системы информационной безопасности объекта персональных данных.
2. Определить уровень защищенности.
3. Определить перечень актуальных угроз.
4. Построить план мероприятий для достижения необходимого уровня защищённости.

Тема «Безопасность персональных данных»

1. С использованием искусственного интеллекта (ИИ) создать документ «Регламент обработки персональных данных».
2. Прокомментируйте пункты регламента предложенные ИИ, укажите что упущено и что учтено, по сравнению с требованиями стандартов.
3. Сделайте выводы по поводу использования систем искусственного интеллекта для создания регламентов.

4. Укажите перечень документов, которые должны входить в нормативную структуру организации-разработчика.

Критерии оценивания заданий

Баллы	1 балл	2 балла	3 балла
Критерий	Задание выполнено частично, требует серьезной доработки	Задание выполнено, но требует некоторой доработки	Задание выполнено полностью, не требует доработки

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)
«Методы и принципы безопасной работы в сети интернет»

1. Аннотация

Дисциплина «Методы и принципы безопасной работы в сети интернет» предназначена для ознакомления слушателей с существующими подходами к построению комплексной защиты компьютерной информации, в том числе автоматизированных систем в защищенном исполнении. В ходе изучения дисциплины слушатели получают знания о современных методах и средствах комплексной защиты информации. Приобретают навыки, необходимые для практического администрирования защищенных компьютерных систем с применением современных средств защиты информации.

Цель дисциплины (результаты обучения)

После освоения дисциплины слушатели смогут:

- Распознавать 99% интернет-угроз (от фальшивых CAPTCHA до поддельных TLS-сертификатов)
- Защищать учетные записи (пароли + 2FA + резервные коды)
- Безопасно работать в публичных сетях (VPN + DNS-over-HTTPS)
- Минимизировать цифровой след (контроль cookies, метаданных)

2. Содержание

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Модуль 3. Методы и принципы безопасной работы в сети интернет (60 часов)			
5.1. Теоретические основы и принципы безопасной работы в сети интернет (20 ч.)	Основные характеристики системы защиты в сети интернет (4 ч.)	Системы защиты (8 ч.). *Задание 1.* Идентификация и контроль доступа, хеширование и Электронная подпись	Изучение систем защиты. Тестирование (10 ч.)
5.2. Каналы утечки информации (20 ч.)	Основные каналы утечки информации в сети интернет (3 ч.)	Механизмы защиты каналов (6 ч.). *Задание 2.* Тестовые испытания каналов защиты: Обеспечение целостности и управление	Изучение каналов защиты. Тестирование (10 ч.)

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
		потоками информации, Шифрование и аудит, дублирование и электронная подпись. Криптопровайдеры. Протокол TLS Антивирусный контроль	
5.3. Методы и средства защиты информации в сети интернет (20 ч.)	Безопасность ценных информационных ресурсов. Выявление конфиденциальных сведений. Носители конфиденциальных сведений. Разработка политики безопасности, концепции безопасности информации, регламента обеспечения безопасности информации, профиля защиты (3 ч.)	Выработка концепции защиты информации (6 ч.). *Задание 3.* Разработка политики безопасности и профиля защиты	Изучение методов средств защиты информации. Тестирование (10 ч.)

3. Условия реализации программы дисциплины

Организационно-педагогические условия реализации программы

Обучение по программе реализовано в формате смешанного обучения, с применением активных технологий совместного обучения в электронной среде (синхронные и асинхронные занятия). Лекционный материал представляется в виде синхронных лекций, записей занятий, текстовых материалов, презентаций, размещаемых в электронном курсе. Данные материалы сопровождаются заданиями и дискуссиями в чатах дисциплин. Изучение теоретического материала (СРС) предполагается до и после синхронной части работы.

Материально-технические условия реализации программы

Синхронные занятия реализуются на базе инструментов видеоконференцсвязи и включают в себя лекционные и практические занятия. Для проведения синхронных занятий (вебинаров со спикерами) применяется программа видеоконференцсвязи. При проведении лекций, практических занятий, самостоятельной работы слушателей используется следующее оборудование: компьютер с наушниками или аудиоколонками, микрофоном и веб-камерой. Программное обеспечение (обновленное до последней версии):

браузер Google Chrome, текстовый редактор. На виртуальных серверах установлено программное обеспечение Inspire, на базе ПК ViPNet, криптопровайдер ViPNet CSP, к которому имеет доступ слушатель через браузер.

Учебно-методическое и информационное обеспечение программы

Дисциплина может быть реализована как очно, так и заочно, в том числе, с применением дистанционных образовательных технологий. Она включает занятия лекционного типа, интерактивные формы обучения, практические занятия.

Содержание комплекта учебно-методических материалов

По данной дисциплине имеется электронный учебно-методический комплекс (УМК) в системе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru/). УМК содержит: систему навигации по дисциплине (учебно-тематический план, интерактивный график работы по дисциплине, сведения о результатах обучения, чат для объявлений и вопросов преподавателю), текстовые материалы к лекциям, практические и тестовые задания, списки основной и дополнительной литературы. В электронном курсе реализована система обратной связи.

Литература

Основная литература

11. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. – М.: ГЛТ, 2016. – 586 с.

12. Емельянова, Н.З. Защита информации в персональном компьютере: учеб. пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – М.: Форум, 2013. – 368 с.

13. Жук А.П. Защита информации: учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. – 392 с.

14. Ищейнов В.Я. Защита конфиденциальной информации: учеб. пособие / В.Я. Ищейнов, М.В. Мецатунян. – М.: Форум, 2013. – 256 с.

15. Малюк А.А. Защита информации в информационном обществе: учеб. пособие для вузов / А.А. Малюк. – М.: ГЛТ, 2015. – 230 с.

16. Платонов В.В. Программно-аппаратные средства защиты информации вычислительных сетей: учеб. пособие: допущено УМО. – М.: Академия, 2007. – 240 с.

17. Хорев П.Б. Программно-аппаратная защита информации: учеб. пособие / П.Б. Хорев. – М.: Форум, 2013. – 352 с.

18. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.

19. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – М.: ДМК Пресс, 2017. – 702 с.

20. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ, НИЦ ИНФРА–М, 2013. – 592 с.

Дополнительная литература

1. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин. – М.: ДМК Пресс, 2011. – 615 с.
2. Защита информации в системах мобильной связи. – М.: Огни, 2014. – 176 с.
3. Защита информации в телекоммуникационных системах / Г.Ф. Конахович и др. – М.: СИНТЕГ, 2014. – 288 с.
4. Золотарев В.В. Программно-аппаратные средства защиты информации: учеб. пособие/ В.В. Золотарев. – Красноярск: СибГАУ, 2007. – 112 с.
5. Малюк, А.А. Введение в защиту информации в автоматизированных системах: учеб. пособие / А.А. Малюк. – М.: Горячая линия – Телеком, 2014. – 148 с.
6. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика; Электроинформ, 2011. – 368 с.
7. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 656 с.
8. Спесивцев А.В. Защита информации в персональных ЭВМ / А.В. Спесивцев, В.А. Вегнер, А.Ю. Крутяков. – М.: Радио и связь,2015. – 192 с.
9. Степанов Е.А. Информационная безопасность и защита информации. учеб. пособие / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2014. – 304 с.
10. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие: Рекомендовано УМО. – М.: Академия, 2007. – 256 с.

Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. Sec.Ru. Интернет портал по безопасности [Электронный ресурс]. – Режим доступа: http://www.sec.ru.
2. SecurityLab.ru [Электронный ресурс]: информационный портал в области защиты информации, интернет права и новых технологий. – Режим доступа: http://www.securitylab.ru.
3. Защита информации и системы безопасности [Электронный ресурс]. – Режим доступа: http://www.runtex.ru.
4. Институт компьютерных технологий [Электронный ресурс]. – Режим доступа: http://www.ict.com.ua.
5. Информационная безопасность [Электронный ресурс]: ООО «Гротек». – Режим доступа: http://www.itsec.ru.
6. Информационная безопасность и защита информации в Российской Федерации (РФ) [Электронный ресурс]. – Режим доступа: http://www.credogarant.ru.
7. Специализированный образовательный портал ТУСУР [Электронный ресурс]. – Режим доступа: http://portal.tusur.ru.
8. Портал БЕЗПЕКА: Все об IT-безопасности. [Электронный ресурс]. – Режим доступа: http://www.bezpeka.com.

4. Оценка качества освоения программы дисциплины (формы аттестации, оценочные и методические материалы)

Форма аттестации по дисциплине — зачет.

Оценка результатов обучения осуществляется следующим образом. Максимально за курс можно набрать 100 %, из них:

- тесты самоконтроля к лекциям 40 %;
- практические задания составляют 60 %.

Зачет получают слушатели, набравшие не менее 50 % из 100 от общего прогресса по курсу.

Примеры тестов для контроля знаний

Пример тестового задания по типу «Множественный выбор»

1. Задачами комплексной защиты информации являются:
   а) явный и скрытый контроль за порядком информационного обмена;
   б) обнаружение вторжений в физическое и информационное пространство;
   в) организация оборота физических носителей информации;
   г) удаление ключевых структур при компрометации.
2. Какие действия попадают под понятие информационных отношений?
   а) распространение;
   б) хранение;
   в) обработка;
   г) разглашение.
3. Программно-математическое воздействие – это воздействие с помощью:
   а) вредоносных программ;
   б) защитных мер;
   в) поиска угроз;
   г) сканирования сети.

Типовое практическое задание

Тема «Теоретические основы и принципы безопасной работы в сети интернет»

Задание

1. Изучение методов конфиденциальной работы в сети интернет.
2. Выбрать один из типов конфиденциальной информации, передаваемых в сети интернет.
3. Разработать методы и предложить средства защиты информации.

РАБОЧАЯ ПРОГРАММА ПРАКТИКИ

1. Аннотация

Основной задачей практики слушателей программы является закрепление в практической деятельности профессиональных компетенций, умений, навыков и знаний, полученных в ходе обучения, а также приобретение необходимых умений и практического опыта на конкретном рабочем месте.

Цель практики — приобретение слушателями программы практического опыта работы, а также освоение новых технологий, форм и методов организации труда непосредственно на рабочем месте.

Планируемые результаты:

По окончании практики слушатели будут способны составлять формализованные описания решений для организации защиты информации организации; разрабатывать организационно-распорядительную документацию на систему защиты информации по формам принятым в организации; разрабатывать техническое задание на проектирование системы защиты информации; определять перечень программно-аппаратных средств защиты информации для обеспечения информационной безопасности; применять выбранные программно-аппаратные средства защиты информации; осуществлять проверку работоспособности программно-аппаратных средств защиты информации; использовать при разработке документации типовые решения и шаблоны, создавать презентации для представления проекта.

2. Содержание

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Практика (16 часов)			
1. Общие вопросы (ознакомление с предприятием)		Ознакомление и изучение конкретной практической задачи (2 ч.)	
2. Практическая часть практики		Решение практической задачи (4 ч.) Интеграция собственного решения в общий проект (2 ч.)	
3. Подготовка отчетной документации			Составление отчета (4 ч.)

Содержание практики включает следующие этапы:

1. Ознакомление с нормативной базой, касающейся охраны труда и правил безопасной работы.

2. Знакомство с рабочим местом и должностными обязанностями, концептом общего тестового проекта.

3. Практическая деятельность, выполняемая под контролем руководителя практики. Обычно включает этапы:

3.1. Формирование отдельной практической задачи по общему проекту;

Содержание практики закрепляется индивидуальным планом прохождения практики (Приложение 1).

Продолжительность практики — 16 часов.

Практика носит индивидуальный или групповой характер и может предусматривать такие виды деятельности как:

- знакомство с предприятием, организационной структурой;
- изучение организации и технологии производства, работ;
- анализ производства;
- Знакомство с проектом;
- работу с технической, нормативной и образовательной документацией;
- составление формализованных описаний решений поставленных задач;
- разработку технического задания на систему защиты информации;
- разработку пакета организационно-распорядительной документации;
- Представление проекта.

3. Условия реализации программы практики

Организационные и педагогические условия реализации программы

Обучение по программе практики реализовано в формате смешанного обучения, с применением активных технологий совместного обучения в электронной среде (синхронные и асинхронные занятия). Материал практических занятий представляется в виде синхронных занятий, презентаций, размещаемых в электронном курсе. Данные материалы сопровождаются заданиями и дискуссиями в чатах дисциплин. Изучение теоретического материала (СРС) предполагается до и после синхронной части работы.

Практика проводится под руководством назначенного руководителя из числа профессорско-преподавательского состава Университета, а также руководителя из состава организации, структурных подразделениях организации, материально-техническое обеспечение которой соответствует профилю программы.

Учебно-методическое и информационное обеспечение

По данному модулю используется электронный УМК. УМК предполагает использование разных типов материалов, сопровождающих учебный процесс,

включая информационные, обучающие и контролирующие. На платформе электронных курсов размещаются задания, приводится перечень необходимых для изучения материалов. Обучающиеся могут на протяжении прохождения практики обращаться к теоретической базе знаний.

4. Оценка качества освоения программы практики (формы аттестации, оценочные и методические материалы)

В качестве подтверждения прохождения практики на базе предприятий, организаций, учреждений, для зачета результатов обучения слушателями предъявляется дневник прохождения практики (Приложение 2) *(отчет в виде дневника прохождения практики)*.

Программу составил:

Канд. физ.-мат наук, доцент,
заведующий кафедрой
информационной безопасности
Института космических
и информационных технологий СФУ  В.И. Вайнштейн

Руководитель программы:

Канд. физ.-мат наук, доцент,
Заведующий кафедрой
информационной безопасности
Института космических
и информационных технологий СФУ  В.И. Вайнштейн

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Наименование образовательной организации

Индивидуальный план слушателя, направляемого на практику

Фамилия, имя, отчество _____
Место работы и должность/статус _____
Название предприятия (организации), где проводится практика
_____
_____
Город _____
Цель практики _____
_____
_____
_____
Срок практики с «____» _____2025 г. по «____» _____2025 г.

План практики

№ п.п.	Перечень разрабатываемых (изучаемых) вопросов, виды работ	Количество часов	Форма отчета
1.			Дневник практики
2.			
3.	Заполнение дневника практики		

СОГЛАСОВАНО

_____ _____ _____
(должность ответственного *(подпись)* *(расшифровка подписи) лица, направляющего на практику)*

Приложение 2

Наименование площадки

УТВЕРЖДАЮ
Руководитель площадки
_____ ФИО
«_____» _____2026 г.
М.П.

ДНЕВНИК
прохождения практики

_____,
(фамилия, имя, отчество специалиста),
проходящего обучение в рамках дополнительной профессиональной программе переподготовки «Разработка мобильных приложений на Unity»

Цель практики:
_____
_____

Руководители практики (от организации): _____
(должность) (ФИО)

1. Дневник

Дата	**Выполняемая работа**	**Вопросы для консультантов и руководителей практики**

2. Краткий отчет о практике

_____
_____
_____
_____
_____
_____
_____

3. Заключение руководителя практики от принимающей организации

_____
_____
_____
_____
_____
_____
_____
_____
_____

Руководитель практики _____ _____
(подпись) (расшифровка подписи)