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

УТВЕРЖДАЮ:
Директор НОЦ «Институт
непрерывного образования
_____ Е.В. Мошкина
«____» _____ 2023 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

«Цифровая безопасность в сети интернет»

Красноярск 2023

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Аннотация программы

Дополнительная профессиональная программа (программа профессиональной переподготовки) ИТ-профиля «Цифровая безопасность в сети интернет» (далее — Программа) разработана в соответствии с нормами Федерального закона РФ от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации»; 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 10.03.01 «Информационная безопасность» (уровень бакалавриата), утвержденного приказом Минобрнауки России от 17 ноября 2020 г. № 1427, (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».

Развитие интернета, нейросетей, машинного обучения и всего, что активно используется в сфере ИТ-безопасности, постепенно начинает быть угрозой. Вредоносные программы становятся всё совершеннее. Количество вредоносного программного обеспечения постоянно растет. Эксперты отмечают, что приблизительно каждые 14 секунд в мире появляется еще одно вредоносное ПО. Сейчас в открытом доступе имеется множество инструкций, а также инструментов для осуществления кибератак. Поэтому, курс профессиональной переподготовки «Цифровая безопасность в сети интернет» всегда будет актуален. Из перечисленного можно сделать вывод, что обеспечение ИТ-безопасности является приоритетным направлением для любого предприятия.

Информационная безопасность обеспечивает защиту данных от несанкционированного доступа посредством программно-аппаратной системы.

Специалисты в этой сфере работы должны уметь проектировать, осуществлять мониторинг, выполнять аттестацию, уметь отлаживать и вводить в эксплуатацию такие вот программно-аппаратные системы защиты.

Перечисление этих знаний и практических навыков говорит о высокой сложности получения такой профессии, не говоря уже о том, что специалисты в этой сфере должны проходить регулярную дополнительную подготовку, так как изменения в этой области очень часто имеют очень сложную конструкцию.

1.2. Цель программы

Цель подготовки слушателей по Программе — формирование у слушателей, обучающихся по специальностям и направлениям подготовки, отнесенным к ИТ-сфере, согласно приложению к Методике расчета показателя «Количество принятых на обучение по программам высшего образования в сфере информационных технологий за счет бюджетных ассигнований федерального бюджета (нарастающим итогом, начиная с 2021 года)», утвержденной приказом Минцифры России от 28 февраля 2022 г. № 143, цифровых компетенций в области информационных технологий, а именно защита информации в автоматизированных системах, а также приобретение по итогам прохождения Программы новой квалификации «Специалист по безопасности компьютерных систем и сетей».

Целевая группа: слушатели, относящиеся к категории обучающихся по специальностям и направлениям подготовки, не отнесенным к ИТ-сфере.

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

1.3.1. 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.

1.3.2. 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.

1.3.3. Уровень квалификации. В соответствии с приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н «Об утверждении Профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», дополнительная профессиональная программа профессиональной переподготовки «Цифровая безопасность в сети интернет» обеспечивает достижение шестого уровня квалификации.

1.3.4. 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		

Трудовые действия	Трудовая функция	Обобщенная трудовая функция	Вид профессиональной деятельности
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 «Цифровая безопасность в сети интернет»

Наименование сферы	**Наименование профессиональной компетенции**	**Пример инструментов**	**0 – способность не проявляется/ проявляется в степени, недостаточной для отнесения к 1 уровню сформированности компетенции**	**1 – способность проявляется под внешним контролем / при внешней постановке задачи/ обучающийся пользуется готовыми, рекомендованными продуктами**	**2 – способность проявляется, но обучающийся эпизодически прибегает к экспертной консультации/ самостоятельно подбирает и пользуется готовыми продуктами**	**3 – способность проявляется системно / обучающийся модифицирует способность под определенные задачи / создает новый продукт, обучает других**
Методы и средства защиты информации	Применяет методы и средства защиты информации для решения профессиональных задач	Криптографические методы, межсетевые экраны	–	+	–	–

1.4. Планируемые результаты обучения

Слушатели в результате освоения программы профессиональной переподготовки «Цифровая безопасность в сети интернет» смогут:

РО1. Определять перечень программно-аппаратных средств защиты информации для обеспечения информационной безопасности.

РО2. Применять выбранные программно-аппаратные средства защиты информации.

РО3. Производить оценку работоспособности применяемых программно-аппаратных средств защиты информации.

РО4. Использовать существующие типовые решения и шаблоны для защиты информации.

РО5. Администрирование средств защиты информации.

1.5. Категория слушателей

Лица, получающие высшее образование по очной (очно-заочной) форме, лица, освоившие основную профессиональную образовательную программу (далее — ОПОП ВО) бакалавриата, в объеме не менее первого курса (бакалавры 2-го курса), ОПОП ВО специалитета — не менее первого и второго курсов (специалисты 3-го курса), обучающиеся по ОПОП ВО, не отнесенным к ИТ-сфере.

1.6. Требования к уровню подготовки поступающего на обучение

В соответствии с требованиями к образованию и обучению, предъявляемыми к 6 уровню квалификации профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», необходимо иметь высшее образование или осваивать его в момент обучения на данной программе.

1.7. Продолжительность обучения

256 часов, из них 128 контактных, в т.ч. 16 часов стажировка.

1.8. Форма обучения

Очно-заочная (обучение по программе реализовано в формате смешанного обучения, с применением электронного обучения и дистанционных образовательных технологий).

1.9. 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 стажировки 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 Google Chrome, Microsoft Visual Studio, GNU GPL v.2. https://git-scm.com/about/free-and-open-source, Blender (GNU General Public License), Unity Education Grant.

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

Особенности построения программы переподготовки «Цифровая безопасность в сети интернет»:

- 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: https://e.sfu-kras.ru/course/view.php?id=35606.

1.11. Особенности организации стажировки

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

Сроки проведения стажировки 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 стажировка осуществляется в форме online стажировки (в формате разработки проекта).

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

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы профессиональной переподготовки
«Цифровая безопасность в сети интернет»

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.	Стажировка	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
«Цифровая безопасность в сети интернет»

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	Результаты обучения
				Лекции	Лабора-торные работы	Практ. и семинарские занятия		
1	**Основы цифровой безопасности**	**96**	**48**	**12**		**36**	**48**	**РО1–РО5**
1.1	Методологические подходы к цифровой безопасности	16	8	2		6	8	РО1–РО5
1.2	Нормативно-правовое регулирование деятельности в области цифровой безопасности	16	8	2		6	8	РО1–РО5
1.3	Основные механизмы цифровой безопасности	16	8	2		6	8	РО1–РО5
2	**Защита персональных данных и безопасность цифрового следа**	**60**	**30**	**10**		**20**	**30**	**РО1–РО5**
2.1	Понятие и виды персональных данных	16	8	2		6	8	РО1–РО5
2.2	Правовой режим персональных данных. Обработка персональных данных	16	8	2		6	8	РО1–РО5
2.3	Безопасность персональных данных	16	8	2		6	8	РО1–РО5
3	**Методы и принципы безопасной работы в сети интернет**	**60**	**30**	**10**		**20**	**30**	**РО1–РО5**
3.1	Теоретические основы и принципы безопасной работы в сети интернет	16	8	1		6	8	РО1–РО5
3.2	Каналы утечки информации	16	8	1		6	8	РО1–РО5
3.3	Методы и средства защиты информации в сети интернет	16	8	2		6	8	РО1–РО5
4	**Стажировка**	**16**	**12**			**12**	**4**	**РО1–РО5**
5	**Итоговая аттестация**	**24**	**8**	**-**		**8**	**16**	**РО1–РО5**
	Всего	**256**	**128**	**32**		**96**	**128**	

Календарный учебный график
дополнительной профессиональной программы профессиональной переподготовки
«Цифровая безопасность в сети интернет»

Наименование модулей (курсов) / Объем учебной нагрузки, ч.	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
Входной ассесмент																																												
Основы информационной безопасности																			К	К																										
Управление информационной безопасностью																																												
Техническая защита информации																																												
Криптографическая защита информации																																												

Комплексная защита информации																																												
Стажировка																																												
Итоговый ассесмент																																												
Итоговая аттестация																																												

II. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

2.1. 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.

2.2. Требования и содержание итоговой аттестации

К итоговой аттестации допускаются слушатели, выполнившие учебный план программы, самостоятельные задания в каждой дисциплине и успешно прошедшие процедуру итогового ассесмента. Итоговая аттестация по программе включает защиту итоговой аттестационной работы (ИАР) в форме проекта, которая проходит в синхронном формате.

Основная цель итоговой аттестационной работы — выполнить работу, демонстрирующую уровень подготовленности к самостоятельной профессиональной деятельности.

ИАР выполняется индивидуально. Защита ИАР включает презентацию работы, вопросы по различным разделам программы. Защита ИАР дает возможность продемонстрировать уровень приобретенных слушателем профессиональных компетенций.

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 «Цифровая безопасность в сети интернет». Объем презентации следует выбирать исходя из длительности выступления (обычно — не более 5–7 минут). В выступлении 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.

Критерии оценивания итоговой аттестационной работы

Итоговая аттестационная работа защищается в синхронном формате перед аттестационной комиссией; работа представляется с помощью устного доклада и демонстрации презентации.

Защита итоговой аттестационной работы является обязательной.

Оценка	Критерии
«Отлично»	− доклад структурирован, полностью раскрывает тему и аргументирует её актуальность; − в докладе чётко обозначены цель и задачи; − докладчик подчёркивает наиболее значимые выводы о проделанной работе; − докладчик показывает перспективы и задачи дальнейшего исследования данной темы; − ответы докладчика на дополнительные вопросы носят чёткий характер и раскрывают сущность поставленных вопросов; − все высказывания докладчика подкрепляются положениями из нормативно – правовых актов, выводами и расчётами; − докладчик использует современные информационные технологии
«Хорошо»	− доклад содержит описание целей и задач, но допускаются неточности при их раскрытии; − при выступлении докладчик, делая выводы, допускает погрешности, которые устраняются в ходе дополнительных уточняющих вопросов; − ответы на дополнительные вопросы раскрывают сущность вопроса, но носят расплывчатый характер; − высказывания докладчика подкрепляются положениями из нормативно – правовых актов, выводами и расчётами; − заключения и выводы недостаточно чётко сформулированы
«Удовлетворительно»	− доклад содержит описание целей и задач, но некоторые из них не достигнуты; − докладчиком допускаются грубые нарушения в логике формулирования выводов; − ответы на дополнительные вопросы носят поверхностный характер; − докладчик слабо подкрепляет выступление положениями из нормативно-правовых актов, выводами и расчётами
«Неудовлетворительно»	− доклад не структурирован; − докладчиком очень слабо раскрыта актуальности темы; − докладчиком не определены цели и задачи; − докладчик допускает грубые логические нарушения в определении выводов; − ответы докладчика на дополнительные вопросы носят поверхностный характер и не раскрывают сущности; − докладчик не подкрепляет свою речь положениями из нормативно – правовых актов, выводами и расчётами

Требования к устному докладу в режиме синхронной защиты

1. Приветствие, обращение к членам комиссии и представление.
2. Тема итоговой аттестационной работы.
3. Актуальность, цель и задачи работы.
4. Анализ результатов работы.
5. Заключение.

Продолжительность выступления — 7–8 минут.

По результатам защиты ИАР аттестационная комиссия принимает решение о присвоении слушателям по результатам освоения дополнительной профессиональной программы профессиональной переподготовки квалификации «Специалист по безопасности компьютерных систем и сетей», о предоставлении права заниматься профессиональной деятельностью в сфере защиты информации в компьютерных системах и сетях и выдаче диплома о профессиональной переподготовке.

III. ОСНОВНОЕ СОДЕРЖАНИЕ ПРОГРАММЫ

3.1. План учебной деятельности

Результаты обучения	Учебные действия/ формы текущего контроля	Используемые ресурсы/ инструменты/технологии
РО1. Определять перечень программно-аппаратных средств защиты информации для обеспечения информационной безопасности	Лекции. Выполнение заданий. Тесты	Материалы электронного курса в системе электронного обучения СФУ «е-Курсы». Видеоконференции
РО2. Применять выбранные программно-аппаратные средства защиты информации	Лекции. Выполнение заданий. Тесты	Материалы электронного курса в системе электронного обучения СФУ «е-Курсы». Видеоконференции
РО3. Производить оценку работоспособности применяемых программно-аппаратных средств защиты информации	Лекции. Выполнение заданий. Тесты	Материалы электронного курса в системе электронного обучения СФУ «е-Курсы». Видеоконференции
РО4. Использовать существующие типовые решения и шаблоны для защиты информации	Лекции. Выполнение заданий. Тесты	Материалы электронного курса в системе электронного обучения СФУ «е-Курсы». Видеоконференции
РО5. Администрирование средств защиты информации	Лекции. Выполнение заданий. Тесты	Материалы электронного курса в системе электронного обучения СФУ «е-Курсы». Видеоконференции

3.2. Виды и содержание самостоятельной работы

Самостоятельная работа слушателя (СРС) предполагает углубление и закрепление теоретических знаний. СРС включает следующие виды самостоятельной деятельности: самостоятельное углубленное изучение вопросов программы, выполнение индивидуальных заданий, подготовка к тестированию и приобретение опыта работы в рамках электронного курса. Выполнение СРС предполагается в дистанционном режиме в рамках электронного курса.

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)
«Основы цифровой безопасности»

1. Аннотация

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

Цель дисциплины (результаты обучения)

По окончании обучения на данной дисциплине слушатели будут способны:

РО1. Определять перечень программно-аппаратных средств защиты информации для обеспечения информационной безопасности.

РО2. Применять выбранные программно-аппаратные средства защиты информации.

РО3. Производить оценку работоспособности применяемых программно-аппаратных средств защиты информации.

РО4. Использовать существующие типовые решения и шаблоны для защиты информации.

РО5. Администрирование средств защиты информации.

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	Федеральные законы по защите информации. Понятие	Нормативно-правовые акты в	Изучение законодательства

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
регулирование деятельности в области цифровой безопасности (32 ч.)	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.)	области информационной безопасности (12 ч.). *Задание 2.* Подготовка презентаций по стандартам в области информационной безопасности	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. 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.)	Изучение средств защиты информации от несанкционированного доступа (12 ч.). *Задание 3.* Настройка элементов политики безопасности с помощью одного из средств защиты информации	Изучение штатных средств операционной системы. Тестирование (16 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.

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 цифровой безопасности»

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 пункта**м 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						
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						

Угроза	Y_1	Y_2	Y	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
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 управления информационной безопасностью, а также развитие у них навыков решения практических задач с применением современных подходов к управлению информационной безопасностью.

Цель дисциплины (результаты обучения)

По окончании обучения на данной дисциплине слушатели будут способны:

РО1. Определять перечень программно-аппаратных средств защиты информации для обеспечения информационной безопасности.

РО2. Применять выбранные программно-аппаратные средства защиты информации.

РО3. Производить оценку работоспособности применяемых программно-аппаратных средств защиты информации.

РО4. Использовать существующие типовые решения и шаблоны для защиты информации.

РО5. Администрирование средств защиты информации.

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	Разработка комплекса мер защиты информации для условной организации

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
		фстэк (6 ч.). *Задание 3*. Исследование информационного объекта, построение плана защиты	(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.

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 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.

Дополнительная литература:

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

1. Подходы к организации информационной безопасности в корпоративных проектах https://infostart.ru/1c/articles/1541897/
2. Информационная безопасность в отраслях: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/informatsionnaya-bezopasnost-v-otraslyakh/
3. БДУ ФСТЭК: 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 сертифицированных средств защиты информации.

Цель дисциплины (результаты обучения)

По окончании обучения на данной дисциплине слушатели будут способны:

РО1. Определять перечень программно-аппаратных средств защиты информации для обеспечения информационной безопасности.

РО2. Применять выбранные программно-аппаратные средства защиты информации.

РО3. Производить оценку работоспособности применяемых программно-аппаратных средств защиты информации.

РО4. Использовать существующие типовые решения и шаблоны для защиты информации.

РО5. Администрирование средств защиты информации.

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	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	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)
		целостности и управление потоками информации, Шифрование и аудит, дублирование и ЭП, 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.

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. 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: Учебное 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: Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. – М.: Форум, 2013. – 256 с.
5. Малюк А.А. Защита информации в информационном обществе: Учебное 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: Учебное 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.

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. Учебное 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 СТАЖИРОВКИ

1. Аннотация

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

Планируемые результаты:

По окончании стажировки 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)
Стажировка (16 часов)			
1. Общие вопросы (ознакомление с предприятием)		Ознакомление и изучение конкретной практической задачи (2 ч.)	
2. Практическая часть стажировки		Решение практической задачи (4 ч.) Интеграция собственного решения в общий проект (2 ч.)	
3. Подготовка отчетной документации			Составление отчета (4 ч.)

Содержание стажировки 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 стажировки. Обычно включает этапы:

3.1. Формирование отдельной практической задачи по общему проекту;

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

Продолжительность стажировки — 16 часов.

Стажировка 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 стажировки

Организационные и педагогические условия реализации программы

Обучение по программе стажировки 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.

Стажировка 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 стажировки обращаться к теоретической базе знаний.

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

В качестве подтверждения прохождения стажировки на базе предприятий, организаций, учреждений, для зачета результатов обучения слушателями предъявляется дневник прохождения стажировки (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 стажировку

Фамилия, имя, отчество _____
Место работы и должность/статус _____
Название предприятия (организации), где проводится стажировка
_____
_____
Город _____
Цель стажировки _____
_____
_____
_____
Срок стажировки с «____» _____2023 г. по «____» _____202 г.

Приказ по вузу от «____» _____202 г. №_____

План стажировки

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

СОГЛАСОВАНО

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

Приложение 2

Наименование стажировочной площадки

УТВЕРЖДАЮ
Руководитель стажировочной площадки
_____ ФИО
«_____» _____2022 г.
М.П.

ДНЕВНИК
прохождения стажировки

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

Цель стажировки:
_____
_____

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

1. Дневник

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

2. Краткий отчет о стажировке

_____
_____
_____
_____
_____
_____
_____

Дата Подпись стажера

3. Заключение руководителя стажировки от принимающей организации

_____
_____
_____
_____
_____
_____
_____
_____
_____

Руководитель стажировки _____ _____
(подпись) (расшифровка подписи)

С заключением руководителя стажировки ознакомлен _____
(подпись стажера)