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

УТВЕРЖДАЮ
Директор НОЦ «Институт
непрерывного образования»
_____ Е.В. Мошкина
«13» ноября 2025 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Современные аспекты информационной безопасности и защиты персональных данных»

Красноярск 2025

УЧЕБНЫЙ ПЛАН
дополнительной профессиональной программы повышения квалификации
«Современные аспекты информационной безопасности и защиты персональных данных»

Форма обучения: очно-заочная, с применением электронного обучения и дистанционных образовательных технологий.
Срок обучения: 72 часа.

№ п/п	Наименование модулей (дисциплин)	Общая трудоем-кость, ч	Всего контактн., ч	Контактные часы		СРС, ч	Формы контроля
				Лекции	Практические и семинарские занятия		
1	Модуль 1. Нормативно-правовое обеспечение информационной безопасности	24	12	4	8	12	Зачет
2	Модуль 2. Защита персональных данных	20	10	2	8	10	Зачет
3	Модуль 3. Основы безопасности в цифровом пространстве	20	10	2	8	10	Зачет
	Итоговая аттестация	**8**	**4**	**-**	**4**	**4**	**Зачет.** ***Итоговое тестирование***
	Итого	**72**	**36**	**8**	**28**	**36**	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
дополнительной профессиональной программы повышения квалификации
«Современные аспекты информационной безопасности и защиты персональных данных»

Категория слушателей: научно-педагогические работники, имеющие опыт работы в образовательных организациях высшего и/или среднего профессионального образования.
Форма обучения: очно-заочная, с применением электронного обучения и дистанционных образовательных технологий.
Режим занятий: 4–6 часов в неделю.

№ п/п	Наименование модулей (курсов)	Общая трудоем-кость, ч	Всего контактн., ч	Контактные часы		СРС, ч	Результаты обучения
				Лекции	Практ. и семинарские занятия		
1	**Модуль 1. Нормативно-правовое обеспечение информационной безопасности**	**24**	**12**	**4**	**8**	**12**	**РО1–РО3**
1.1	Тема 1.1. Виды информации, защищаемой на законном основании	12	6	2	4	6	РО1–РО2
1.2	Тема 1.2. Нормативно-правовое регулирование деятельности в области цифровой безопасности	12	6	2	4	6	РО1–РО3
2	**Модуль 2. Защита персональных данных**	**20**	**10**	**2**	**8**	**10**	**РО2–РО4**
2.1	Тема 2.1. Понятие и виды персональных данных	10	5	2	3	5	РО2–РО4
2.2	Тема 2.2. Безопасность персональных данных	10	5	2	3	5	РО1–РО4
3	**Модуль 3. Основы безопасности в цифровом пространстве**	**20**	**10**	**2**	**8**	**10**	**РО2–РО4**
3.1	Тема 3.1. Актуальные угрозы в цифровом пространстве	10	5	2	3	5	РО2–РО4
3.2	Тема 3.2. Основы противодействия злоумышленникам в цифровом пространстве	10	5	2	3	5	РО2–РО4
	Итоговая аттестация	**8**	**4**		**4**	**4**	**РО1–РО4**
	Итого	**72**	**36**	**8**	**28**	**36**	

Календарный учебный график
дополнительной профессиональной программы повышения квалификации
«Современные аспекты информационной безопасности и защиты персональных данных»

Наименование модулей (курсов)	Неделя	Объем учебной нагрузки, ч.	Виды занятий (количество часов)			
			Лекции	Практ. и семинарские занятия	СРС	Итоговый контроль
Модуль 1. Нормативно-правовое обеспечение информационной безопасности	1–4	24	4	8	12	Зачет
Модуль 2. Защита персональных данных	5–6	20	2	8	10	Зачет
Модуль 3. Основы безопасности в цифровом пространстве	7–8	20	2	8	10	Зачет
Итоговая аттестация	**9**	**8**		**4**	**4**	**Зачет**

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Аннотация программы

Стремительное развитие сетевых и информационных технологий наблюдается на протяжении последнего десятилетия, что способствует появлению значимых изменений во всех областях общественной жизни и отраслях. Усиление роли технологий неизбежно ведет к возникновению рисков, связанных с обеспечением информационной и в частности цифровой безопасности информации, и побуждает к необходимым своевременным корректировкам ее защиты как со стороны специалистов в области информационной безопасности, так и со стороны пользователей современных информационных технологий.

Равно как и «цифровая гигиена», так и умение обезопасить себя в цифровом пространстве — необходимые знания современного человека. А постоянное развитие навыков в данной сфере является необходимым условием, поскольку информационные технологии совершенствуются, происходит масштабное развитие Интернета, нейросетей, машинного обучения и всего, что активно используется в сфере ИТ-безопасности, а количество вредоносного программного обеспечения постоянно растет.

Для профессорско-преподавательского состава высших учебных заведений также необходимо владеть как минимум базовыми знаниями в области информационной безопасности для обеспечение безопасного образовательного процесса в ВУЗе, в частности, основами цифровой безопасности в сети Интернет. Поэтому, дополнительная профессиональная программа повышения квалификации «Современные аспекты информационной безопасности и защиты персональных данных» всегда будет актуальна.

1.2. Цель программы

Цель подготовки слушателей по Программе — формирование у слушателей компетенций в области информационных технологий, а именно защиты информации.

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

Программа повышения квалификации разработана на основе квалификационных характеристик должностей руководителей и специалистов высшего профессионального и дополнительного профессионального образования, утвержденных приказом Минздравсоцразвития РФ от 11.01.2011 г. № 1н (Единый квалификационный справочник должностей руководителей, специалистов и служащих (ЕКСД), редакция от 09.04.2018 г.), и соответствует требованиям Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Минобрнауки России от 1 июля 2013 г. № 499, приказа Минобрнауки России от 29 марта 2019 г. № 178, а также с учетом прогноза научно-технологического развития Российской Федерации до 2030 года.

Программа направлена на совершенствование компетенций (совершенствование способов и средств исполнения должностных обязанностей в соответствии с указанным выше разделом ЕКСД) в части «Должности профессорско-преподавательского состава»:

– организация и осуществление учебной и учебно-методической работы по преподаваемой дисциплине или отдельным видам учебных занятий;

– организация и планирование методического и цифрового дидактического обеспечения учебных занятий;

– защита информации в компьютерных системах и сетях.

1.4. Планируемые результаты обучения

Слушатели в результате освоения дополнительной профессиональной программы повышения квалификации «Современные аспекты информационной безопасности и защиты персональных данных» 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.

1.5. Категория слушателей

Научно-педагогические работники, реализующие образовательные программы высшего и/или дополнительного профессионального образования; административно-управленческий персонал СФУ.

1.6. Требования к уровню подготовки поступающего на обучение

Необходимо иметь среднее профессиональное или высшее образование.

1.7. Продолжительность обучения

72 часа, из них 36 контактных.

1.8. Форма обучения

Заочная, асинхронный формат (с применением электронного обучения и дистанционных образовательных технологий).

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

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

При проведении лекций, практических занятий, самостоятельной работы слушателей 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, текстовый редактор, редактор презентаций.

1.10. Особенности (принципы) построения дополнительной профессиональной программы повышения квалификации

Особенности построения дополнительной профессиональной программы повышения квалификации «Современные аспекты информационной безопасности и защиты персональных данных»:

– в основу проектирования программы положен компетентностный подход;

– выполнение учебных заданий, требующих практического применения знаний и умений, полученных в ходе изучения логически связанных дисциплин;

– использование информационных и коммуникационных технологий, в том числе современных систем технологической поддержки процесса обучения, обеспечивающих комфортные условия для обучающихся, преподавателей;

– применение электронных образовательных ресурсов.

В поддержку дополнительной профессиональной программы профессиональной переподготовки разработан электронный курс: https://e.sfu-kras.ru/course/view.php?id=38142.

1.11. Документ об образовании: удостоверение о повышении квалификации установленного образца.

II. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Обучение по программе реализовано в формате смешанного обучения, с применением активных технологий дистанционного обучения в электронной среде (асинхронные занятия). Лекционный материал представляется в виде комплекса мини-видеолекций, 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. Реализация самостоятельной работы (СРС), а также выполнение практических заданий предполагается посредством изучения и выполнения соответствующих материалов, размещаемых в системе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru).

Учебно-методическое и информационное обеспечение дисциплины

По программе разработан электронный учебно-методический комплекс (УМК) — электронный курс в системе электронного обучения СФУ «е-Курсы».

Содержание комплекта учебно-методических материалов

Учебно-методический комплекс содержит: систему навигации по программе, 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

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.

III. КАДРОВЫЕ УСЛОВИЯ

Руководитель программы:

***Вайнштейн Виталий Исаакович**, кандидат физико-математических наук, заведующий кафедрой информационной безопасности Института космических и информационных технологий Сибирского федерального университета.*

Преподаватели программы:

***Лазарева Виктория Александровна,** старший преподаватель кафедры информационной безопасности Института космических и информационных технологий Сибирского федерального университета.*

***Шиманович Роман Сергеевич,** старший преподаватель кафедры информационной безопасности Института космических и информационных технологий Сибирского федерального университета.*

IV. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

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

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.

3.2. Программное обеспечение (информационные обучающие системы, системы вебинаров, сетевые ресурсы хостинга видео, изображений, файлов, презентаций и др.)

Лекционный материал представляется в виде комплекса мини-видеолекций, 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. Реализация самостоятельной работы (СРС), а также выполнение практических заданий предполагается посредством изучения и выполнения соответствующих материалов, размещаемых в системе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru).

V. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

5.1. Формы аттестации, оценочные материалы, методические материалы

Программа предусматривает проведение промежуточной и итоговой аттестации в формате тестирования. Обучение на программе повышения квалификации предполагает также выполнение индивидуальных текущих заданий, тестирование.

Итоговое тестирование включает вопросы каждого пройденного модуля программы.

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

Для успешного завершения программы повышения квалификации требуется выполнить итоговое тестирование.

Основанием для аттестации слушателя по данной программе является:

− выполнение на положительную оценку всех текущих заданий, размещенных в электронном образовательном курсе;

− выполнение итогового теста.

Критерии оценивания

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

− тесты самоконтроля к лекциям и итоговое тестирование — 40 %;

− практические задания составляют 60 %.

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

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)
«Современные аспекты информационной безопасности и защиты персональных данных»

1. Аннотация

Дополнительная профессиональная программа повышения квалификации «Современные аспекты информационной безопасности и защиты персональных данных» 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.

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.

2. Содержание

Наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Модуль 1. Нормативно-правовое обеспечение информационной безопасности (24 ч.)			
Тема 1.1. Виды информации, защищаемой на законном основании (12 ч.)	Основные понятия и термины. Политика информационной безопасности. Стратегия национальной безопасности РФ. Понятие модели нарушителя информационной безопасности (2 ч.)	Моделирование угроз информационной безопасности (4 ч.)	Изучение политик информационной безопасности. Тестирование (6 ч.)
Тема 1.2. Нормативно-правовое регулирование деятельности в области цифровой безопасности (12 ч.)	Федеральные законы по защите информации. Понятие и виды защищаемой информации. Юридическая ответственность в области информационной безопасности (2 ч.)	Нормативно-правовые акты в области информационной безопасности (4 ч.)	Изучение законодательства РФ в области защиты информации. Тестирование (6 ч.)

Наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Модуль 2. Защита персональных данных (20 ч.)			
Тема 2.1. Понятие и виды персональных данных (10 ч.)	ПДн понятия и виды (2 ч.)	План защиты ПДн (3 ч.)	Изучение видов ПДн и создание плана защиты. Тестирование (5 ч.)
Тема 2.2. Безопасность персональных данных (10 ч.)	ПДн и единые требования к построению модели угроз и нарушителя (2 ч.)	Практика построения модели угроз на основе методики ФСТЭК (3 ч.)	Разработка комплекса мер защиты информации для условной организации. Тестирование (5 ч.)
Модуль 3. Основы безопасности в цифровом пространстве (20 ч.)			
Тема 3.1. Актуальные угрозы в цифровом пространстве (10 ч.)	Основные характеристики системы защиты в сети Интернет (2 ч.)	Системы защиты (3 ч.)	Изучение систем защиты. Тестирование (5 ч.)
Тема 3.2. Основы противодействия злоумышленникам в цифровом пространстве (10 ч.)	Безопасность ценных информационных ресурсов. Выявление конфиденциальных сведений. Носители конфиденциальных сведений. (2 ч.)	Выработка концепции защиты информации. Разработка политики безопасности и профиля защиты (3 ч.)	Изучение методов защиты информации. Тестирование (5 ч.)
Итоговая аттестация (8 ч.)			
Зачет (8 ч.)	–	Практические задания (4 ч)	Итоговое тестирование (4 ч.)

3. Оценка качества освоения программы модулей (формы аттестации, оценочные и методические материалы)

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

– тесты самоконтроля к лекциям и итоговое тестирование — 40 %;

– практические задания составляют — 60 %.

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

Примеры тестовых заданий

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.

4. Для чего используются DCAP системы?

а) для автоматизированного аудита файлов и данных в ИС, поиска нарушений при обращении с конфиденциальной информацией;

б) для аккумулирования данных из разных сканеров безопасности и систем обнаружения атак;

в) для мониторинга состояния сетевого оборудования, используемого в ИС;

г) для сбора и анализа событий безопасности из разных источников обеспечения и контроля информационной безопасности ИС.

5. Свойство информации, которое указывает на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, называется:

а) доступностью информации;

б) адекватностью информации;

в) целостностью информации;

г) конфиденциальностью информации.

6. Потенциальная опасность для информации или системы — это:

а) угроза;

б) уязвимость;

в) воздействие;

г) риск.

7. 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.

8. Какие действия попадают под понятие информационных отношений?

а) распространение;

б) хранение;

в) обработка;

г) разглашение.

Типовое практическое задание

Тема «Нормативно-правовое обеспечение информационной безопасности»

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

Тема «Защита 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.

Тема «Основы безопасности в цифровом пространстве»

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.

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

Программу составили:

Старший преподаватель кафедры
информационной безопасности ИКИТ _____ В.А. Лазарева

Старший преподаватель кафедры
информационной безопасности ИКИТ _____ Р.С. Шиманович

Руководитель программы:

Заведующий кафедрой
информационной безопасности ИКИТ _____ В.И. Вайнштейн