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

УТВЕРЖДАЮ
Директор НОЦ «Институт
непрерывного образования»
_____ Е.В. Мошкина
«__» марта 2024 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Защита объектов критической информационной инфраструктуры»

Красноярск 2024

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Аннотация программы

Уровень зависимости процессов современного предприятия от бесперебойной работы его информационных систем сегодня как никогда высок. Паралич информационных систем социально значимого предприятия может оставить город/регион без воды, газа и электроэнергии. Нарушение работы транспортной отрасли может привести к коллапсу целых городов.

Программа повышения квалификации направлена на знакомство слушателей с современной проблематикой информационной безопасности объектов критической информационной инфраструктуры (КИИ) и ее аспектами, актуальными в масштабе предприятий и организаций; приобретение и углубление знаний в области методологии информационной безопасности, правового, организационного и технического обеспечения, в т.ч. особенностями защиты информации в компьютерной и сетевой среде, защиты речевой информации, защиты персональных данных, коммерческой и служебной тайны.

Информационная безопасность обеспечивает защиту программ и данных от несанкционированного доступа посредством программных и программно-аппаратных средств информационной безопасности.

Специалисты в этой сфере работы должны уметь обеспечивать необходимый уровень защищенности автоматизированных систем, функционирующих в условиях существования угроз в информационной сфере и обладающих информационно-технологическими ресурсами, подлежащими защите, используемых в том числе на объектах критической информационной инфраструктуры, в отношении которых отсутствует необходимость присвоения им категорий значимости.

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 программы повышения квалификации — формирование и(или) совершенствование профессиональных компетенций в сфере комплексного обеспечения информационной безопасности на предприятиях критической информационной инфраструктуры, освоение механизмов обеспечения информационной безопасности, изучение практических решений управления информационной безопасностью с учетом современных тенденций в постоянно развивающейся области защиты информации.

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

В соответствии с профессиональным стандартом 06.033 «Специалист по защите информации в автоматизированных системах» (утвержден приказом

Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н), можно выделить следующие трудовые функции на формирование и совершенствование которых направлена программа повышения квалификации (6-ой уровень квалификации):

A/01.5 Техническое обслуживание программно-аппаратных средств защиты информации в операционных системах.

A/02.5 Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях.

A/03.5 Техническое обслуживание средств защиты информации прикладного и системного программного обеспечения.

B/01.6 Администрирование подсистем защиты информации в операционных системах.

B/02.6 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях.

1.4. Планируемые результаты обучения

Слушатели в результате освоения программы повышения квалификации «Защита объектов критической информационной инфраструктуры» смогут:

РО1. Проводить оценку эффективности комплекса технических и организационных мер обеспечения информационной безопасности объекта критической информационной инфраструктуры.

РО2. Проводить проверки работоспособности системы защиты информации автоматизированной системы.

РО3. Участвовать в оценке и обработке рисков информационной безопасности объекта критической информационной инфраструктуры.

РО4. Планировать построение и поддержание системы информационной безопасности объекта критической информационной инфраструктуры на требуемом уровне.

РО5. Применять требования регуляторов при подборе технических средств защиты информации на объектах критической информационной инфраструктуры и применении компенсирующих мер.

1.5. Категория слушателей

Лица, получающие высшее образование по очной (очно-заочной) форме, лица, освоившие образовательную программу бакалавриата, в объеме не менее первого курса (бакалавры 2-го курса), образовательную программу специалитета — не менее первого и второго курсов (специалисты 3-го курса).

1.6. Требования к уровню подготовки поступающего на обучение

Среднее профессиональное или высшее образование.

Необходимо свободное владение компьютером, базовыми интернет-технологиями (системы искусственного интеллекта, поиск, электронная почта).

1.7. Продолжительность обучения: 144 часа, из них 72 контактных, 72 часа — самостоятельная практическая работа.

1.8. Форма обучения: очно-заочная 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 в системе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru/). При проведении лекций, практических занятий, самостоятельной работы слушателей используется 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 Yandex, системы SberJazz, Яндекс-Телемост, сервис видеоконференций СФУ https://i.sfu-kras.ru/conference/.

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

Особенности построения программы повышения квалификации «Защита объектов критической информационной инфраструктуры» в рамках Инженерного образовательного центра:

– все занятия, кроме самостоятельных работ, проводятся дистанционно в синхронном и асинхронном режиме;

– в основу проектирования программы положен компетентностный подход;

– учебные задания требуют практического применения знаний и умений, полученных в ходе изучения лекционного и практического материала;

– требуется выполнение итоговых работ по реальному заданию;

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

– используются электронные образовательные ресурсы (дистанционное, электронное, комбинированное обучение и пр.).

В поддержку программы повышения квалификации разработан электронный курс в системе электронного обучения СФУ «е-Курсы»: https://e.sfu-kras.ru/course/.

1.11. Документ об образовании: удостоверение повышения квалификации установленного образца.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
программы повышения квалификации
«Защита объектов критической информационной инфраструктуры»

Категория слушателей: лица, имеющие/получающие высшее образование в области информационной безопасности.
Срок обучения: 12 недель.
Форма обучения: очно-заочная с использованием электронного обучения и дистанционных образовательных технологий.
Режим занятий: 3 раза в неделю, 2 часа в день.

№ п/п	Наименование и содержание разделов и тем программы	Общая трудоем-кость, ч	Всего контактн., ч	Контактные часы:		СРС, ч.	Использование средств ЭО и ДОТ	Результаты обучения
				Лекции	Практ. и семинарские занятия			
1	**Модуль 1. Организационное и правовое обеспечение информационной безопасности КИИ**	32	16	6	10	16		**РО1–РО5**
1.1	Система обеспечения информационной безопасности	6	3	1	2	3	Электронный курс в системе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru/)	РО1
1.2	Основы теории правового обеспечения информационной безопасности	6	3	1	2	3		РО1, РО2
1.3	Юридическая ответственность за нарушения в области информационной безопасности	6	3	1	2	3		РО1, РО3
1.4	Организационные системы обеспечения безопасности информации	6	3	1	2	3		РО2, РО4
1.5	Правила категорирования объектов КИИ. Требования регуляторов	6	3	1	2	3		РО1, РО2, РО5
1.6	Корпоративное нормативное регулирование	2	1	1	2	1		РО3, РО4, РО5
2	**Модуль 2. Криптографическая защита информации КИИ**	36	18	6	12	18		**РО1–РО5**
2.1	Основные понятия и история криптографии	12	6	2	4	6		РО1, РО2

№ п/п	Наименование и содержание разделов и тем программы	Общая трудоем-кость, ч	Всего контактн., ч	Контактные часы:		СРС, ч.	Использование средств ЭО и ДОТ	Результаты обучения
				Лекции	Практ. и семинарские занятия			
2.2	Применение средств криптографической защиты информации в КИИ	12	6	2	4	6	Электронный курс в системе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru/)	РО1, РО2, РО3
2.3	Системы шифрования, криптографические протоколы, типы и виды СКЗИ	12	6	2	4	6		РО3, РО4, РО5
3	**Модуль 3. Программные и аппаратные средства защиты информации КИИ**	36	18	6	12	18		**РО1–РО5**
3.1	Особенности обеспечения информационной безопасности КИИ	12	6	2	4	6	Электронный курс в системе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru/)	РО1, РО2, РО3
3.2	Уровни значимости защищаемых информационных объектов и виды средств защиты	12	6	2	4	6		РО1, РО4, РО5
3.3	Построение модели угроз на объектах КИИ	12	6	2	4	6		РО2, РО3, РО4, РО5
4	**Модуль 4. Безопасность компьютерных сетей**	36	18	6	12	18		**РО1–РО5**
4.1	Сетевые технологии, их уязвимости и типовые атаки	12	6	2	4	6	Электронный курс в системе электронного обучения СФУ «е-Курсы» (https://e.sfu-kras.ru/)	РО3, РО4, РО5
4.2	Средства защиты информации сетевой инфраструктуры	12	6	2	4	6		РО1, РО2, РО5
4.3	Методология защиты компьютерных сетей	12	6	2	4	6		РО1, РО2, РО3, РО4
	Итоговая аттестация	**4**	**2**			**2**		**РО1–РО5**
	ИТОГО	**144**	**72**			**72**		

II. ОСНОВНОЕ СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. План учебной деятельности

Результаты обучения	Учебные действия/ формы текущего контроля	Используемые ресурсы/ инструменты/технологии
РО1. Проводить оценку эффективности комплекса технических и организационных мер обеспечения информационной безопасности объекта критической информационной инфраструктуры	Лекции. Самостоятельный анализ информационных материалов. Выполнение заданий. Тестирование	Материалы электронного курса в системе ЭО СФУ «е-Курсы». Онлайнресурсы: БИК СФУ, eLIBRARY.RU. Видеоконференции
РО2. Проводить проверки работоспособности системы защиты информации автоматизированной системы.	Лекции. Самостоятельный анализ информационных материалов. Выполнение заданий. Тестирование	Материалы электронного курса в системе ЭО СФУ «е-Курсы». Онлайнресурсы: БИК СФУ, eLIBRARY.RU. Видеоконференции
РО3. Участвовать в оценке и обработке рисков информационной безопасности объекта критической информационной инфраструктуры	Лекции. Самостоятельный анализ информационных материалов. Выполнение заданий. Тестирование	Материалы электронного курса в системе ЭО СФУ «е-Курсы». Онлайнресурсы: БИК СФУ, eLIBRARY.RU. Видеоконференции
РО4. Планировать построение и поддержание системы информационной безопасности объекта критической информационной инфраструктуры на требуемом уровне	Лекции. Самостоятельный анализ информационных материалов. Выполнение заданий. Тестирование	Материалы электронного курса в системе ЭО СФУ «е-Курсы». Онлайнресурсы: БИК СФУ, eLIBRARY.RU. Видеоконференции
РО5. Применять требования регуляторов при подборе технических средств защиты информации на объектах критической информационной инфраструктуры и применении компенсирующих мер	Лекции. Самостоятельный анализ информационных материалов. Выполнение заданий. Тестирование	Материалы электронного курса в системе ЭО СФУ «е-Курсы». Онлайнресурсы: БИК СФУ, eLIBRARY.RU. Видеоконференции

2.2. Виды и содержание самостоятельной работы

Для обеспечения программы разработаны учебно-методические материалы по всем модулям и темам программы в формате электронного обучающего курса.

Для организации самостоятельной работы (изучения теоретического материала, учебно-методических материалов для проведения практических занятий, нормативных актов), слушателям предоставляется доступ к системе электронного обучения СФУ «е-Курсы» (http://e.sfu-kras.ru) (логин, пароль), предусматривающий возможность изучения и скачивания необходимых презентационных, учебно-методических и нормативных материалов, осуществления обратной связи и контактов с преподавателями программы

Электронный образовательный курс содержит: презентации занятий, материалы для самостоятельного изучения, диагностические инструменты, иллюстрирующие видеоматериалы, ссылки на законодательные акты по теме программы.

III. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

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

1. Банк данных угроз безопасности информации содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов. – URL: http://bdu.fstec.ru/.
2. Баранова Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. – М.: Риор, 2018. – 400 с.
3. ГОСТ Р ИСО/МЭК 27007-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности».
4. Компьютерная справочная правовая система в России, содержит свыше 102 миллионов документов. – URL: http://www.consultant.ru/.
5. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty.
6. Официальный сайт государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (госСОПКА). – URL: http://gossopka.ru/.
7. Партыка Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. – М.: Форум, 2021. – 432 с. – URL: https://www.ibooks.ru/bookshelf/359939/reading.
8. Постановление Правительства РФ № 127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры РФ и их значений».
9. Постановление Правительства РФ № 162 от 17.02.2018 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры РФ».
10. Приказ ФСБ России № 366 от 24.07.2018 «О Национальном координационном центре по компьютерным инцидентам».
11. Приказ ФСБ России № 367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА».
12. Приказ ФСБ России № 196 от 06.05.2019 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».
13. Приказ ФСБ России № 281 от 19.06.2019 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для

обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации».

14. Приказ ФСБ России № 368 от 24.07.2018 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».

15. Приказ ФСТЭК России № 227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры РФ».

16. Приказ ФСТЭК России № 229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности ЗО КИИ РФ».

17. Приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности ЗО КИИ РФ и обеспечению их функционирования».

18. Приказ ФСТЭК России № 236 от 21.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

19. Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности ЗО КИИ РФ».

20. Прохорова О.В. Информационная безопасность и защита информации / О.В. Прохорова. – Самара: СГАСУ (Самарский госуд. архит.-строит. ун-т), 2019. – 114 с.

21. Указ Президента РФ № 646 от 05.12.2016 «Об утверждении Доктрины информационной безопасности Российской Федерации».

22. Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации».

23. Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации. – URL: http://cert.gov.ru/.

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

Площадкой реализации программы является система электронного обучения СФУ «е-Курсы» (http://e.sfu-kras.ru).

IV. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

4.1. Формы аттестации, оценочные материалы, методические материалы

Программа предусматривает проведение текущей и итоговой аттестации. Текущая аттестация слушателей проводится на основе оценки выполнения практических заданий в электронном обучающем курсе, выполнения индивидуальных текущих заданий.

Методические материалы, необходимые для выполнения текущих заданий, представлены в соответствующих разделах электронного обучающего курса и включают текстовые, презентационные, графические и видео материалы, методические рекомендации по выполнению заданий.

Контроль результатов обучения по программе включает в себя:

– промежуточную аттестацию в рамках практических занятий — презентация проектов, анализа конкретных ситуаций, рассматриваемых в рамках проведения киберучений и диагностических упражнений;

– итоговую аттестацию — тестирование.

Примеры тестовых заданий к лекциям

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.

Примеры практических заданий

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						
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

4.2. Требования и содержание итоговой аттестации

Основанием для аттестации является выполнение итогового online тестирования в рамках электронного обучающего курса в системе электронного обучения СФУ. Оценка выставляется по шкале «зачтено не зачтено».

Для проведения аттестации разработан банк тестовых заданий, по всем темам программы повышения квалификации.

Банк тестовых заданий составляет 200 тестовых вопросов.

Итоговый тест в электронной системе обучения СФУ включает в себя 20 вопросов по всем модулям программы.

Тестирование ограничено по времени, результаты демонстрируются слушателям непосредственно сразу после окончания итоговой аттестации.

Для получения оценки «зачтено» слушателю необходимо набрать не менее 65 % верных ответов в итоговом тесте.

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