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

УТВЕРЖДАЮ
Директор НОЦ «Институт
непрерывного образования»
_____ Е.В. Мошкина
«20» июня 2024 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОЙ ПЕРЕПОДГОТОВКИ

«Методы противодействия угрозам в цифровом пространстве»

Красноярск 2024

I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Аннотация программы

Дополнительная профессиональная программа (программа профессиональной переподготовки) ИТ-профиля «Методы противодействия угрозам в цифровом пространстве» (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 06.033 «Специалист по защите информации в автоматизированных системах», 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 06.033 «Специалист по защите информации в автоматизированных системах».

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 «Методы противодействия угрозам в цифровом пространстве» 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 защите информации в автоматизированных системах».

Целевая группа: слушатели, относящиеся к категории обучающихся по специальностям и направлениям подготовки, 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 защите информации в автоматизированных системах», дополнительная профессиональная программа профессиональной переподготовки «Методы противодействия угрозам в цифровом пространстве» 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 06.033 «Специалист по защите информации в автоматизированных системах», 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
Проверка работоспособности системы защиты информации автоматизированной системы	A/01.5 Проведение регламентных работ по эксплуатации систем защиты информации автоматизированных систем	A Обслуживание систем защиты информации в автоматизированных системах	Обеспечение безопасности информации в автоматизированных системах
Контроль соответствия конфигурации системы защиты информации автоматизированной системы её эксплуатационной документации			
Ведение документов учета, обработки, хранения и передачи информации, составляющей тайну	A/02.5 Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем		
Информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации			
Уничтожение информации, обрабатываемой автоматизированной системой	A/03.5 Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем		
Обнаружение инцидентов в процессе эксплуатации автоматизированной системы	B/01.6 Диагностика систем защиты информации автоматизированных систем	B Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации	

Трудовые действия	Трудовая функция	Обобщенная трудовая функция	Вид профессиональной деятельности
Обеспечение безопасности информации с учетом требования эффективного функционирования автоматизированной системы	B/02.6 Администрирование систем защиты информации автоматизированных систем		
Составление комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	B/03.6 Управление защитой информации в автоматизированных системах		

Таблица 2

Характеристика новой и развиваемой цифровой компетенции в ИТ-сфере, связанной с уровнем формирования и развития в результате освоения программы «Методы противодействия угрозам в цифровом пространстве»

Наименование сферы	**Наименование профессиональной компетенции**	**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 принципы информационной безопасности	–	Участвует в проектах по ИБ в составе команды под контролем опытных специалистов	–	–
Методы и средства защиты информации	Применяет программное обеспечение для защиты информации	–	Администрирует тиражные системы по защите информации. Настраивает и использует системы под контролем опытных специалистов	–	–
Методы и средства защиты информации	Применяет средства криптографической защиты информации		Использует уже настроенные средства криптографической защиты информации, может изменять параметры при наличии строго сформулированной задачи		

1.4. Планируемые результаты обучения

Слушатели в результате освоения программы профессиональной переподготовки «Методы противодействия угрозам в цифровом пространстве» 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 разработки руководящих документов по защите информации в организации.

РО5. Разрабатывать требования к организации защиты информации в организации.

РО6. Применять международные стандарты информационной безопасности.

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, отнесенным к ИТ-сфере.

1.6. Требования к уровню подготовки поступающего на обучение

Среднее специальное или высшее образование, или осваивать его в момент обучения на данной программе.

1.7. Продолжительность обучения

360 часов, из них 180 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 «Методы противодействия угрозам в цифровом пространстве»:

- 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 «Методы противодействия угрозам в цифровом пространстве» 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
«Методы противодействия угрозам в цифровом пространстве»

Форма обучения – очно-заочная.
Срок обучения – 360 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 информационной безопасности	64	32	8		24	32	Зачет
2.	Управление информационной безопасностью	64	32	8		24	32	Зачет
3.	Техническая защита информации	64	32	6		26	32	Зачет
4.	Криптографическая защита информации	64	32	8		24	32	Зачет
5.	Комплексная защита информации	64	32	6		26	32	Зачет
6.	Стажировка	16	12			12	4	Зачет
7.	Итоговая аттестация	24	8			8	16	Защита итоговой аттестационной работы (проекта)
	Итого	**360**	**180**	**36**		**144**	**180**	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
дополнительной профессиональной программы профессиональной переподготовки
«Методы противодействия угрозам в цифровом пространстве»

Категория слушателей: лица, имеющие или получающие среднее специальное или высшее образование.
Срок обучения: 360 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 информационной безопасности**	**64**	**32**	**8**		**24**	**32**	**РО1–РО5**
1.1	Методологические подходы к защите информации и принципы ее организации	16	8	2		6	8	РО1–РО5
1.2	Правовое, нормативное и методическое регулирование деятельности в области защиты информации	16	8	2		6	8	РО1–РО5
1.3	Основные механизмы защиты информации	16	8	2		6	8	РО1–РО5
1.4	Обеспечение безопасности информационных систем с помощью средств защиты информации	16	8	2		6	8	РО1–РО5
2	**Управление информационной безопасностью**	**64**	**32**	**8**		**24**	**32**	**РО1–РО6**
2.1	Основы построения системы управления информационной безопасностью (СУИБ)	16	8	2		6	8	РО1–РО6
2.2	Особенности построения СУИБ для различных категорий защищаемой информации	16	8	2		6	8	РО1–РО6
2.3	Анализ рисков, построение модели угроз	16	8	2		6	8	РО1–РО6
2.4	Безопасность приложений, требования к разработке и построению СУИБ	16	8	2		6	8	РО1–РО6
3	**Техническая защита информации**	**64**	**32**	**6**		**26**	**32**	**РО1–РО5**
3.1	Теоретические основы, принципы и способы добывания информации	16	8	1		6	8	РО1–РО5
3.2	Технические каналы утечки информации	16	8	1		6	8	РО1–РО5

№ 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		
3.3	Технические разведки. Методы и средства технической разведки	16	8	2		6	8	РО1–РО5
3.4	Техническая защита информации на объектах информатизации	16	8	2		8	8	РО1–РО5
4	**Криптографическая защита информации**	**64**	**32**	**8**		**24**	**32**	**РО1–РО5**
4.1	Основные понятия и история криптографии. Модели шифров	16	8	2		6	8	РО1–РО5
4.2	Симметричные алгоритмы. Криптографические хэш-функции	16	8	2		6	8	РО1–РО5
4.3	Системы шифрования с открытыми ключами	16	8	2		6	8	РО1–РО5
4.4	Электронная подпись. Криптографические протоколы	16	8	2		6	8	РО1–РО5
5	**Комплексная защита информации**	**64**	**32**	**6**		**26**	**32**	**РО1–РО5**
5.1	Физическая защита информации	16	8	1		6	8	РО1–РО5
5.2	Программно-аппаратный уровень защиты информации	16	8	1		6	8	РО1–РО5
5.3	Организационно-режимная защита информации	16	8	2		6	8	РО1–РО5
5.4	Комплексная защита информации — сущность, задачи, стратегии	16	8	2		8	8	РО1–РО5
6	**Стажировка**	**16**	**12**			**12**	**4**	**РО1–РО5**
7	**Итоговая аттестация**	**24**	**8**	**-**		**8**	**16**	**РО1–РО5**
	Всего	**360**	**180**	**36**		**144**	**180**	

Календарный учебный график
дополнительной профессиональной программы профессиональной переподготовки
«Методы противодействия угрозам в цифровом пространстве»

Наименование модулей (курсов) Объем учебной нагрузки, ч.	2024-25 учебный год																																										
	сентябрь					октябрь					ноябрь				декабрь				январь				февраль				март				апрель				май					июнь					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
Входной ассесмент																																												
Основы информационной безопасности																																											
Промежуточный ассессмент																																											
Управление информационной безопасностью																			К	К																								
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, успешно прошедшие процедуру итогового ассесмента. Итоговая аттестация по программе включает представление итоговой аттестационной работы (ИАР) в форме проекта. Основная цель итоговой аттестационной работы— выполнить работу, демонстрирующую уровень подготовленности к самостоятельной профессиональной деятельности.

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

Критерии оценивания итоговой аттестационной работы

Оценка	Критерии
«Отлично»	− ИАР структурирована, полностью раскрывает тему и аргументирует её актуальность; − в ИАР чётко обозначены цель и задачи; − в ИАР приведены наиболее значимые выводы о проделанной работе; − в ИАР отражены перспективы и задачи дальнейшего исследования данной темы; − все выводы подкрепляются положениями из нормативно – правовых актов и расчётами; − в ИАР использованы современные информационные технологии
«Хорошо»	− ИАР содержит описание целей и задач, но допускаются неточности при их раскрытии; − все выводы подкрепляются положениями из нормативно – правовых актов и расчётами; − заключения и выводы недостаточно чётко сформулированы
«Удовлетворительно»	− ИАР содержит описание целей и задач, но некоторые из них не достигнуты; − допускаются грубые нарушения в логике формулирования выводов; − выводы, приведенные в ИАР слабо подкреплены положениями из нормативно-правовых актов, выводами и расчётами

По результатам выполнения ИАР аттестационная комиссия принимает решение о присвоении слушателям по результатам освоения дополнительной профессиональной программы профессиональной переподготовки квалификации «Специалист по защите информации в автоматизированных системах», 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 разработки руководящих документов по защите информации в организации	Лекции. Выполнение заданий. Тесты	Материалы электронного курса в системе электронного обучения СФУ «е-Курсы». Видеоконференции
РО5. Разрабатывать требования к организации защиты информации в организации	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 информационной безопасности»

1. Аннотация

Дисциплина «Основы информационной безопасности» предназначена для изучения принципов информационной безопасности государства, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного 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 разработки руководящих документов по защите информации в организации.

РО5. Разрабатывать требования к организации защиты информации в организации.

2. Содержание

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Модуль 1. Основы информационной безопасности (64 часа)			
1.1. Методологические подходы к защите информации и принципы ее организации (16 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 (2 ч.)	Моделирование угроз информационной безопасности (6 ч.) *Задание 1*. Определение актуальных угроз безопасности при обработке персональных данных в информационной системе	Изучение политик информационной безопасности. Тестирование (8 ч.)
1.2. Правовое, нормативное и	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)
методическое регулирование деятельности в области защиты информации (16 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» (2 ч.)	области информационной безопасности (6 ч.). *Задание 2.* Подготовка презентаций по стандартам в области информационной безопасности	РФ в области защиты информации. Тестирование (8 ч.)
1.3. Основные механизмы защиты информации (16 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 (2 ч.)	Изучение средств защиты информации от несанкционированного доступа (6 ч.). *Задание 3.* Настройка элементов политики безопасности с помощью одного из средств защиты информации	Изучение штатных средств операционной системы. Тестирование (8 ч.)

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
1.4. Обеспечение безопасности информационных систем с помощью средств защиты информации (16 ч.)	Средства защиты информации от НСД. Основные функции. Схемы применения. Аппаратные модули доверенной загрузки. Основные функции. Схемы применения. Системы обнаружения вторжений. Основные функции. Схемы применения Средства антивирусной защиты информации. Основные функции. Схемы применения. Межсетевые экраны. Основные функции. Схемы применения. Средства криптографической защиты информации. Основные функции. Схемы применения. SIEM. Основные функции. Схемы применения. Системы анализа защищенности. Основные функции. Схемы применения. Защита среды виртуализации. Основные функции. Схемы применения. DLP. Основные функции. Схемы применения. (2 ч.).	Анализ программных средств защиты информации (6 ч.). *Задание 4.* Разработка проекта защиты информационной системы с помощью средств защиты информации	Анализ программных средств защиты информации. Тестирование (8 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 защите информации и принципы ее организации»

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

Заполнить таблицы:

Таблица 1 – Определение уровня исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;	–	–	+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);	–	–	+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;	–	+	–
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;	–	+	–
локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;	–	–	+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;	–	+	–
ИСПДн, физически отделенная от сети общего пользования	+	–	–
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+	–	–
запись, удаление, сортировка;	–	+	–
модификация, передача	–	–	+
4.По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	**Средний**	**Низкий**
ИСПДн с открытым доступом	–	–	+
5. *По наличию соединений с другими базами ПДн иных ИСПДн:*			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);	–	–	+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн	+	–	–
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+	–	–
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;	–	+	–
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)	–	–	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;	–	–	+
ИСПДн, предоставляющая часть ПДн;	–	+	–
ИСПДн, не предоставляющая никакой информации	+	–	–
Итого			

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

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

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

$$Y_1 =$$

Таблица 2 – Определение перечня актуальных угроз

Угроза	Y_1	Y_2	Y	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
Угрозы утечки ПДн по техническим каналам						
Утечка информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН)						
Утечка акустической (речевой) информации						
Утечка видовой информации						

Угроза	Y_1	Y_2	Y	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
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

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)
«Управление информационной безопасностью»

1. Аннотация

Дисциплина «Управление информационной безопасностью» 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 разработки руководящих документов по защите информации в организации.

РО5. Разрабатывать требования к организации защиты информации в организации.

РО6. Применять международные стандарты информационной безопасности.

2. Содержание

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Модуль 2. Управление информационной безопасностью (64 часа)			
2.1. Основы построения системы управления информационной безопасностью (СУИБ) (16 ч.)	СУИБ как часть общей системы управления предприятия (2 ч.)	Стандарт ISO 27001 (6 ч.). *Задание 1.* Построение плана создания СУИБ на основе ГОСТ Р ИСО\МЭК 2700х	Изучение стандартов группы ГОСТ Р ИСО\МЭК 2700х. Тестирование (8 ч.)
2.2. Особенности построения СУИБ для различных категорий защищаемой информации (16 ч.)	Категории защищаемой информации в рамках законодательства РФ (2 ч.)	Законодательные и организационные основы построения СУИБ для информационных объектов коммерческой тайны, ИСПДн, ГИС.	Изучение схем построения. Тестирование (8 ч.)

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
		Требования к субъектам КИИ (6 ч.). *Задание 2.* Описание сил и средств СУИБ для субъекта КИИ, на основе приказа ФСТЭК №135	
2.3. Анализ рисков и построение модели угроз (16 ч.)	СУИБ и единые требования к построению модели угроз (2 ч.)	Практика построения модели угроз на основе методики ФСТЭК, особенности использования БДУ фстэк (6 ч.). *Задание 3*. Исследование информационного объекта, построение плана защиты	Разработка комплекса мер защиты информации для условной организации (оператора ПДн, владельца коммерческой тайны, оператора ГИС либо субъекта КИИ, по выбору). Тестирование (8 ч.)
2.4. Безопасность приложений, требования к разработке и построению СУИБ (16 ч.)	Безопасная разработка приложений в контексте построения и поддержания СУИБ, требования к разработчикам, защита информации на уровне приложений в организациях с учётом построения СУИБ (2 ч.).	Обеспечение выполнения СУИБ в организации – разработчике ПО, обеспечить требуемый уровень доверяя для заказчика (6 ч.) *Задание 4* Разработать регламент безопасной разработки.	Изучение методов безопасной разработки приложений, информационных систем, с учётом требований стандарта ГОСТ Р ИСО\МЭК 27034, требований регуляторов (заказчики: оператор ПДн, банк, оператор ГИС, субъект КИИ, и пр. по выбору) (8 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 ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения. Общие требования. – М.: Стандартинформ, 2016. – 26 с.

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

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

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

5 ГОСТ Р ИСО/МЭК 27003-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной

безопасности. Руководство по реализации системы менеджмента информационной безопасности. – М.: Стандартинформ 2021. – 38 с.

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

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

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

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

10 Управление информационной безопасностью: 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.

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

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

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

Форма аттестации по дисциплине — зачет.

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

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

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

Примеры тестов для контроля знаний

Пример тестового задания по типу «Множественный выбор»

1. Для чего используются DCAP системы?
   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.

2. 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.

3. Потенциальная опасность для информации или системы — это:
а) угроза;
б) уязвимость;
в) воздействие;
г) риск.

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

1. Составить отчёт об обследовании системы информационной безопасности объекта КИИ.
2. Определить категорию значимости.
3. Определить перечень актуальных угроз.
4. Построить план мероприятий для достижения необходимого уровня защищённости.

Тема «Безопасность приложений, требования к разработке и построению СУИБ»

1. С использованием искусственного интеллекта (ИИ) создать документ «Регламент разработки безопасного программного обеспечения» согласно цикла SSDLC.
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 по безопасной разработке.
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)
«Техническая защита информации»

1. Аннотация

Дисциплина «Техническая защита информации» предназначена для ознакомления слушателей с принципами построения и особенностям функционирования средств технической защиты информации, включает в себя методы защиты информации. В результате изучения дисциплины у слушателей должны сформироваться знания, умения и навыки, позволяющие проводить самостоятельный анализ физических процессов, происходящих в технических средствах защиты информации, как изучаемых в настоящей дисциплине, так и находящихся за ее рамками.

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 разработки руководящих документов по защите информации в организации.

РО5. Разрабатывать требования к организации защиты информации в организации.

2. Содержание

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Модуль 3. Техническая защита информации (64 часа)			
3.1. Теоретические основы, принципы и способы добывания информации (16 ч.)	Цели и задачи инженерно-технической защиты информации. Виды информации, защищаемой техническими средствами. Физические эффекты в технических системах. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Основные и вспомогательные технические средства, и системы. Способы	Изучение свойств физических полей, электрических сигналов и материальных тел как носителей информации (6 ч.)	Изучение способов доступа к источникам информации ограниченного доступа. Тестирование (8 ч.)

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
	доступа к источникам информации ограниченного доступа. Наблюдение, перехват, подслушивание (1 ч.)		
3.2. Технические каналы утечки информации (16 ч.)	Понятие и особенности утечки информации по техническим каналам. Структура канала утечки. Виды каналов утечки. Условия образования каналов утечки. Характеристики каналов утечки информации. Акустические, оптические, радиоэлектронные и материально-вещественные каналы утечки информации. Методы защиты от утечки информации (1 ч.)	Акустический и виброакустический каналы утечки информации (6 ч.)	Изучение каналов утечки. Тестирование (8 ч.)
3.3. Технические разведки. Методы и средства технической разведки (16 ч.)	Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Возможности видов технической разведки. Основные направления развития технической разведки. Методы и средства технической разведки. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Генераторы линейного и пространственного зашумления (2 ч.)	Технические средства для поиска закладных устройств (6 ч.)	Изучение методов технической разведки. Тестирование (8 ч.)
3.4. Техническая защита информации на объектах информатизации (16 ч.)	Государственная система противодействия технической разведке: основные задачи и структура. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке. Основные организационные и технические меры по защите информации. Организация работ по инженерно-технической защите на	Методы и средства активной и пассивной защиты от утечек информации по техническим каналам (8 ч.)	Изучение нормативных и методических документов. Тестирование (8 ч.)

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
	предприятиях. Основные инженерные конструкции. Методы скрытия информации и ее носителей. Контроль эффективности мер по защите информации техническими средствами (2 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. Зайцев А.П. Технические средства и методы защиты информации. – М.: Машиностроение, 2019. – 508 с. [Электронный ресурс]. – Режим доступа: http://window.edu.ru/resource/611/63611.
2. Сидорин Ю.С. Технические средства защиты информации: учеб. пособие. – СПб.: Изд-во СПбГПУ, 2005. – 141 с. [Электронный ресурс]. – Режим доступа: http://window.edu.ru/resource/593/29593.
3. Царегородцев А.В. Технические средства защиты информации: учебник. – М.: Изд-во ВГНА Минфина России, 2009 (доступ из электронной библиотеки СФУ).
4. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М: ФОРУМ, 2013. – 592 с. (доступ из электронной библиотеки СФУ).

Дополнительная литература

1. Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей. – М.: Изд-во Горячая Линия-Телеком, 2008.
2. Гришина Н.В. Организация комплексной системы защиты информации. – М.: Изд-во Гелиос АРВ, 2007.
3. Железняк В.К. Защита информации от утечки по техническим каналам. – СПб.: Изд. ГУАП, 2006.
4. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. – М.: Изд-во Горячая Линия-Телеком, 2006.
5. Курило А.П., Зефиров С.Л., Голованов В.Б. Аудит информационной безопасности. – М.: Изд-во БДЦ-Пресс, 2006.
6. Петраков А.В. Основы практической защиты информации. – М.: СОЛОН-Пресс, 2005.
7. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учеб. пособие. – М.: Изд-во Academia, 2006.
8. Сидорин Ю.С. Технические средства защиты информации: учеб. пособие. – СПб.: Изд-во Политехн. ун-та, 2005.
9. Соболев А.Н., Кириллов В.М. Физические основы технических средств обеспечения информационной безопасности. – М.: Гелиос АРВ, 2004.
10. Торокин А.А. Инженерно-техническая защита информации: учебное пособие. – М.: Изд-во Гелиос АРВ, 2005.
11. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

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

1. Официальный сайт федеральной службы по техническому и экспортному контролю [Электронный ресурс]. – Режим доступа: http://fstec.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 100 %;

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. По какому каналу можно осуществить перехват информации?
   а) акустическому;
   б) беспроводному;
   в) оптическому;
   г) типовому.
2. Нарушители, не имеющие доступа к ИС, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена называются:
   а) сильными нарушителями;
   б) внешними нарушителями;
   в) внутренними нарушителями;
   г) инсайдерами.
3. Для защиты от утечки информации по видовому каналу могут применяться:
   а) расположение монитора так, чтобы в окно не был виден экран;
   б) генераторы акустического шума;
   в) физическая охрана помещений;
   г) жалюзи на окнах.

Типовое практическое задание

Практические задания по дисциплине «Техническая защита информации» являются демонстрационными, каждое из которых включает в себя:

– Теоретическую часть, материал которой излагается преподавателем в начале занятия.

– Демонстрационную часть, в ходе которой преподаватель описывает и демонстрирует возможности специальных технических средств (в рамках конкретного практического занятия), которые в силу их высокой стоимости могут быть приобретены в единичном количестве.

– Практическую часть, в ходе которой студенты лично знакомятся со специальными техническими средствами и выполняют индивидуальное задание преподавателя.

№ п/п	№ раздела дисциплины	Наименование занятий
1	1	Ознакомление с возможностями многофункционального поискового устройства
1	1	Оценка защищённости ограждающих конструкций помещения от утечки информации по акустическому и виброакустическому каналам
2	2	Ознакомление с закладными устройствами, принципами их проектирования, камуфлирования и работы
3	3	Ознакомление с методикой поиска работающих активных закладных устройств
4	4	Ознакомление с методикой поиска выключенных активных закладных устройств
5	4	Ознакомление с методикой обнаружения устройств сетевых закладок
6	4	Ознакомление с методикой предотвращения утечки информации по электромагнитному каналу посредством пространственного зашумления
7	4	Ознакомление с принципами работы электронных замков

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)
«Криптографическая защита информации»

1. Аннотация

Дисциплина «Криптографическая защита информации» предназначена для ознакомления слушателей с общими принципами построения и использования криптографических методов для защиты информации, а также развитие у них навыков решения практических задач с применением современных криптографических методов. Данная дисциплина должна дать студентам представления о современных методах и моделях криптографии, принципах криптостойкости и криптоанализа шифров и научить практическим навыкам анализа криптосистем посредством компрометации шифров и алгоритмов.

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 разработки руководящих документов по защите информации в организации.

РО5. Разрабатывать требования к организации защиты информации в организации.

2. Содержание

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Модуль 4. Криптографическая защита информации (64 часа)			
4.1. Основные понятия и история криптографии. Модели шифров (16 ч.)	Место криптографии в сфере научных знаний. Криптосистемы. Задачи криптоанализа. Алфавит открытых сообщений. Частотные характеристики текстовых сообщений. Шифры замены и перестановка (2 ч.)	Классические симметричные шифры (6 ч.). *Задание 1.* Реализация шифров Атбаш, Цезаря, Ришелье, Виженера	Изучение моделей и алгоритмов симметричного шифрования. Тестирование (8 ч.)
4.2. Симметричные алгоритмы.	Криптоанализ классических шифров. Гаммирование. Методы генерации	Криптоанализ классических шифров (6 ч.).	Изучение методов криптоанализа

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Криптографические хэш-функции (16 ч.)	псевдослучайных чисел. Стандарт шифрования DES, AES, ГОСТ. Атаки на блочные шифры. Шифры с переменной длиной ключа. Поточные шифры. Алгоритмы безопасного хэширования (2 ч.)	*Задание 2.* Частотный криптоанализ. Криптоанализ полиалфавитных шифров	классических шифров. Тестирование (8 ч.)
4.3. Системы шифрования с открытыми ключами (16 ч.)	Асимметричные криптосистемы. Односторонние функции. Криптосистема RSA, Эль-Гамаля. Метод ключевого обмена Диффи-Хелмана. Алгоритмы практической реализации криптосистем с открытым ключом. Криптография на основе эллиптических кривых. Блокчейн (2 ч.)	Асимметричная криптография (6 ч.). *Задание 3.* Реализация криптосистем RSA, Эль-Гамаля, метода ключевого обмена Диффи-Хелмана	Изучение асимметричных криптосистем. Тестирование (8 ч.)
4.4. Электронная подпись. Криптографически е протоколы (16 ч.)	Электронная подпись в различных криптосистемах. Алгоритмы электронной подписи: RSA, ESGA, DSA, ГОСТ. Управление ключами. Генерация, Резервирование, Распределение. Управление. Атаки на ЦС. Криптографические протоколы. Основные задачи, современные системы (2 ч.)	Схемы электронной подписи (6 ч.). *Задание 4.* Реализация алгоритмов электронной подписи: RSA, Эль-Гамаля, ГОСТ, FIPS	Изучение схем электронной подписи. Тестирование (8 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. Бабаш А.В. Криптографические методы защиты информации: учебно-метод. пособие для студентов вузов, обучающихся по специальности 080801 «Прикладная информатика» и другим междисциплинарным специальностям / А.В. Бабаш. Т. 2. – М., 2014.

2. Васильева И.Н. Криптографические методы защиты информации: учебник и практикум для академического бакалавриата по инженерно-техническим направлениям и специальностям / И.Н. Васильева; Санкт-Петербург. гос. эконом. ун-т. – СПб., 2018.

3. Гашков С.Б. Криптографические методы защиты информации: учеб. пособие для студентов вузов / С.Б. Гашков, Э.А. Применко, М.А. Черепнев. – М., 2010.

4. Рябко Б.Я. Криптографические методы защиты информации: Рекомендовано УМО по образованию в области телекоммуникаций в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям: «Многоканальные телекоммуникационные системы»,

«Радиосвязь, радиовещание и телевидение», «Защищенные системы связи» / Рябко Б.Я.; Фионов А.Н. – М., 2012.

Дополнительная литература

1. Авдошин С. Набебин А. Дискретная математика. Модулярная алгебра, криптография, кодирование. – М., 2017. – 352 с.
2. Адаменко М. Основы классической криптологии. Секреты шифров и кодов. – М., 2016. – 296 с.
3. Зуев Ю. По океану дискретной математики. От перечислительной комбинаторики до современной криптографии. Том 1. – М., 2017. – 274 с.
4. Зуев Ю. По океану дискретной математики. От перечислительной комбинаторики до современной криптографии. Том 2. – М., 2017. – 370 с.
5. Панасенко С. Алгоритмы шифрования. Специальный справочник. – М., 2009. – 576 с.
6. Применко Э. Алгебраические основы криптографии. – М., 2015. – 284 с.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С (Applied Cryptography: Protocols, Algorithms and Source Code in C). – М., 2016. – 1024 с.
8. Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography (2nd edition) – Chapman & Hall/CRC Cryptography and Network Security Series, 2008.
9. Paar C., Pelzl J. Understanding Cryptography. A Textbook for Students and Practitioners. – Springer, 2010.
10. Nigel Smart. Cryptography: An Introduction. (3rd Edition) – 2009. – URL: (https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf).

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

1. The cryptopals crypto challenges. URL: http://cryptopals.com.
2. IEEE Computer Society'sTechnical Committeeon Security and Privacy. URL: http://www.ieee-security.org/.

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. Симметричные шифры подразделяются на шифры:
   а) перестановки;
   б) с открытым ключом;
   в) с закрытым ключом;
   г) подстановки.
2. Какой из перечисленных шифров является шифром сложной замены?
   а) шифр Гронсфельда;
   б) шифр Атбаш;
   в) магические квадраты;
   г) шифр Цезаря.
3. Отметить методы, которые позволяются найти длину ключевого слова полиалфавитного шифра:
   а) Метод индекса совпадений;
   б) Автокорреляционный метод;
   в) Метод Касиски;
   г) Все вышеперечисленные.

Типовое практическое задание

Тема «Симметричные алгоритмы. Криптографические хэш функции)»

Цель работы: получение практических навыков в криптоанализе зашифрованного теста на основе частотного анализа.

Задание: Необходимо реализовать метод частотного анализа шифртекста.

1. Написать программу нахождения частоты символов в текстовом файле.
2. Построить гистограммы частоты встречаемости символов текста.
3. Произвести криптоанализ приведенного ниже текста на английском языке.

GB OR, BE ABG GB OR: GUNG VF GUR DHRFGVBA:
JURGURE 'GVF ABOYRE VA GUR ZVAQ GB FHSSRE
GUR FYVATF NAQ NEEBJF BS BHGENTRBHF SBEGHAR,
BE GB GNXR NEZF NTNVAFG N FRN BS GEBHOYRF,
NAQ OL BCCBFVAT RAQ GURZ? GB OVR: GB FYRRC;
AB ZBER; NAQ OL N FYRRC GB FNL JR RAQ
GUR URNEG-NPUR NAQ GUR GUBHFNAQ ANGHENY FUBPXF
GUNG SYRFU VF URVE GB, 'GVF N PBAFHZZNGVBA
QRIBHGYL GB OR JVFU'Q, GB QVR, GB FYRRC;
GB FYRRC: CREPUNAPR GB QERNZ: NL, GURER'F GUR EHO;
SBE VA GUNG FYRRC BS QRNGU JUNG QERNZF ZNL PRZR
JURA JR UNIR FUHSSYRQ BSS GUVF ZBEGNY PBVY,
ZHFG TVIR HF CNHFR: GURER'F GUR ERFCRPG
GUNG ZNXRF PNYNZVGL BS FB YBAT YVSR;

4. Произвести криптоанализ приведенного ниже текста на русском языке.

«ХФ ЬЭМЧЯХДСЮЧХВ ЮЫЫНЭМУСЪХЦ ОМУЪЫ ЫНСЮЬСДХЯИ
СРХЪЮЯОЫ ЧЭХЯСЭХСО ЫГСЪЧХ ЬЭЫРАЧЯЫО Х ЮХЮЯСЩ

ЪМЬЭХЩСЭ ДЯЫНЗ ЫНШСПДХЯИ ЫГСЪЧА ЮХЮЯСЩЗ ЮЫЮЯМОШСЪЪЫЦ ХФ ЭМЪСС ЮСЭЯХБХГХЭЫОМЪЪЗВ ЬЭЫРАЧЯЫЮ ЬЫ ЙЯЫЦ ЬЭХДХЪС РШЛ ЮХЮЯСЩ Х ЬЭЫРАЧЯЫЮ ООЫРХЯЮЛ СРХЪЗЦ ЯСЭЩХЪ ЫНЖСЧЯ ЫГСЪЧХ ЧМУРМЛ ЮХЮЯСЩМ Х ХШХ ЬЭЫРАЧЯ ЬЭСРЖЛОШЛСЯ ЮОЫХ ЯЭСНЫОМЪХЛ Ч ЫНСЮЬСДСЪХК ЧЫЪБХРСЪГХМШИЪЫЮЯХ ГСШЫЮЯЪЫЮЯХ Х РЫЮЯАЬЪЫЮЯХ ДЯЫНЗ АРЫОШСЯОЫЭХЯИ ЙЯХ ЯЭСНЫОМЪХЛ ЪСЫНВЫРХЩЫ ЬЭСРЫЮЯМОХЯИ ЮЫЫЯОСЯЮЯОАКЁХЦ ЪМНЫЭ БАЪЧГХЦ ЮСЭОХЮЫО НСФЫЬМЮЪЫЮЯХ ЯМЧХВ ЧМЧ ХРСЪЯХБХЧМГХЛ Х МАЯСЪЯХБХЧМГХЛ АЬЭМОШСЪХС РЫЮЯАЬЫЩ ХШХ ОЫЮЮЯМЪЫОШСЪХС ЬЫЮШС ЮНЫСО».

Интерфейс программы должен быть графический.

Описание метода:

Частотный анализ, частотный криптоанализ — один из методов криптоанализа, основывающийся на предположении о существовании статистического распределения отдельных символов и их последовательностей как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.

Упрощённо, частотный анализ предполагает, что частота появления заданной буквы алфавита в достаточно длинных текстах одна и та же для разных текстов одного языка. При этом в случае моноалфавитного шифрования если в шифротексте будет символ с аналогичной вероятностью появления, то можно предположить, что он и является указанной зашифрованной буквой.

Приблизительные частоты распределения букв уже давно составлены практически для всех языков мира (см. таблицы распределения букв).

Алгоритм для подсчета частоты появления символов алфавита в блоке исходного текста:

На первом шаге вводится символы исходного текста из файла в массив символов. Файл, содержащий исходный текст, должен иметь текстовый формат. Одновременно определяем принадлежность вводимого символа к множеству букв используемого алфавита или цифр. Если введенный символ не является таковым, то исключаем его из рассмотрения.

В дальнейшем для всех букв/цифр просматриваем массив и подсчитываем число появлений каждой из них, а также определяем относительные частоты появления букв по формуле: (частота появления i-го символа/общее количество символов текста)*100. После чего для криптоанализа и сравним их со среднестатистическими.

Достоверность получаемых в ходе эксперимента относительных частот повышается с увеличением размерности анализируемого блока текста.

Также необходимо принимать во внимание особенности текста (например, литературный или технический), для которых относительные частоты букв могут несколько различаться.

Таблица 1 – Распределение вероятностей букв в русских текстах

Буква	Вероятность	Буква	Вероятность	Буква	Вероятность	Буква	Вероятность
Пробел	0,175	Р	0,040	Я	0,018	Х	0,009
О	0,090	В	0,038	Ы	0.016	Ж	0,007
Е	0,072	Л	0,035	З	0,016	Ю	0,006
А	0,062	К	0,028	Ъ	0,014	Ш	0,006
И	0,062	М	0,026	Б	0,014	Ц	0,004
Н	0,053	Д	0,025	Г	0,013	Щ	0,003
Т	0,053	П	0,023	Ч	0,012	Э	0,003
С	0,045	У	0,021	Й	0,010	Ф	0,002

Таблица 2 – Распределение вероятностей букв в английских текстах

Буква	Вероятность	Буква	Вероятность	Буква	Вероятность
E	0,123	L	0,040	B	0,016
T	0,096	D	0,036	G	0,016
A	0,081	C	0,032	V	0,009
O	0,079	U	0,031	K	0,005
N	0,072	P	0,023	Q	0,002
I	0,071	F	0,023	X	0,002
S	0,066	M	0,022	J	0,001
R	0,060	W	0,020	Z	0,001
H	0,051	Y	0,019		

РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)
«Комплексная защита информации»

1. Аннотация

Дисциплина «Комплексная защита информации» 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 разработки руководящих документов по защите информации в организации.

РО5. Разрабатывать требования к организации защиты информации в организации.

2. Содержание

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
Модуль 5. Комплексная защита информации (64 часа)			
5.1. Физическая защита информации (16 ч.)	Основные характеристики системы физической защиты. Силы реагирования. Права и обязанности должностных лиц караула. Пропускной и внутриобъектовый режимы. Технические и инженерные средства охраны (2 ч.)	Физическая защита (6 ч.) *Задание 1* Идентификация и контроль доступа	Изучение систем физической защиты. Тестирование (8 ч.)

№, наименование темы	Содержание лекций (кол-во часов)	Наименование практических (семинарских занятий) (кол-во часов)	Виды СРС (кол-во часов)
5.2. Программно – аппаратная защита информации (16 ч.)	Проведение комплексного обследования защищенности ИС. Состав работ по проведению аудита (2 ч.).	Механизмы защиты (8 ч.). *Задание 2* Тестовые испытания механизмов защиты: Обеспечение целостности и управление потоками информации, Шифрование и аудит, Дублирование и ЭП, Антивирусный контроль	Изучение механизмов защиты. Тестирование (8 ч.)
5.3. Организационно-распорядительная защита информации (16 ч.)	Безопасность ценных информационных ресурсов. Выявление конфиденциальных сведений. Носители конфиденциальных сведений. Разработка политики безопасности, концепции безопасности информации, регламента обеспечения безопасности информации, профиля защиты (1 ч.)	Разработка документов (6 ч.). *Задание 3* Разработка политики безопасности и профиля защиты	Изучение конфиденциального делопроизводства. Тестирование (8 ч.)
5.4. Комплексная защита информации — сущность, задачи, стратегии (16 ч.)	Сущность и задачи комплексной защиты информации. Этапы построения КЗИ для различных стратегий (1 ч.)	Этапы построения КЗИ (6 ч.). *Задание 4* Реквизиты конфиденциального документа	Изучение этапов построения КЗИ. Тестирование (8 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: учеб. пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. – М.: Форум, 2013. – 368 с.,

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

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

5. Малюк А.А. Защита информации в информационном обществе: 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: учеб. пособие / П.Б. Хорев. – М.: Форум, 2013. – 352 с.
8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.
9. Шаньгин В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. – М.: ДМК Пресс, 2017. – 702 с.
10. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах: учеб. пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ, НИЦ ИНФРА–М, 2013. – 592 с.

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 «Общая характеристика комплексной защиты информации»

Задание

1. Изучить реквизиты конфиденциального документа.
2. Выбрать один из типов документов, разрабатываемых в рамках мероприятий по защите информации (Технический паспорт, акт классификации и т.п.).
3. Разработать конфиденциальный документ с учетом всех реквизитов конфиденциальности, таких как:

- учетный номер;
- гриф конфиденциальности;
- количество экземпляров;
- дата отпечатывания;
- исполнитель;
- другие реквизиты.

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 (6 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 «____» _____2024 г. по «____» _____2024 г.

Приказ по вузу от «____» _____2024 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
«_____» _____2024 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)