Государственное бюджетное учреждение
дополнительного профессионального педагогического образования
центр повышения квалификации специалистов
«Информационно-методический Центр»
Адмиралтейского района Санкт-Петербурга

190005, Санкт-Петербург, наб. р. Фонтанки, д. 134 б (литер А)
Телефон: 251-59-79, 251-01-62, факс 251-59-79
e-mail: imc@adm-edu.spb.ru

«ПРИНЯТО»
Педагогическим советом
Образовательного учреждения
Протокол от _____ № __

«УТВЕРЖДЕНО»
Приказом от _____ № _____

Врио директора_____М.С. Новиков

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
(повышение квалификации)

«ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГОСУДАРСТВЕННЫХ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ»

Направление: Организационно-управленческие дефициты
Количество часов: **36 ч.**

Санкт-Петербург
2024

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Актуальность программы объясняется необходимостью оказания информационной, методической и организационной поддержки руководителям, заместителям руководителя и специалистам образовательных учреждений в обеспечении эффективной реализации мероприятий по информационной безопасности в образовательном учреждении.

В современных условиях развития новых технологий, информационных и телекоммуникационных инфраструктур происходит формирование и увеличение новых угроз, связанных с информационной безопасностью. Поэтому вопрос о необходимости целенаправленной подготовки квалифицированных кадров в области информационной безопасности является крайне актуальным.

Таким образом, программа повышения квалификации направлена на рассмотрение основных видов угроз информационной безопасности и методов защиты данных, а так же существующие, перспективные решения вопроса подготовки специалистов, соответствующих современным стандартам информационной безопасности, и ликвидацию организационно-управленческих, психолого-педагогических дефицитов у руководителей, заместителей руководителей образовательных учреждений по обеспечению информационной безопасности.

Цель:

Повышение профессиональной компетенции слушателей в организации мероприятий по информационной безопасности на уровне образовательной организации.

Задачи:

- ознакомить с нормативно-методическими основами информационной безопасности на уровне образовательного учреждения;
- определение угроз информационной безопасности;
- формирование требований к обеспечению информационной безопасности данных при их обработке, к системе защиты данных;
- выбор организационных и технических мер, а также реализуемых ими мероприятий по обеспечению информационной безопасности данных при их обработке в информационных системах;
- внедрение организационных и технических мер, а также реализуемых ими мероприятий по обеспечению информационной безопасности данных при их обработке в информационных системах;
- разработка и внедрение системы защиты данных;
- установка, настройка, испытания и техническое обслуживание программных (программно-аппаратных) средств защиты информации;
- обеспечение информационной безопасности данных в ходе эксплуатации;
- обеспечение информационной безопасности данных при выводе из эксплуатации в информационных системах.

Планируемые результаты:

Освоение программы позволит руководителю, заместителю руководителя, специалисту ответственному за обеспечение информационной безопасности:

- использовать нормативные правовые акты, методические документы в области обеспечения информационной безопасности данных при их обработке в информационных системах и национальные стандарты в области защиты информации в своей деятельности;
- использовать достижения науки и техники, пользоваться реферативными и справочно-информационными изданиями в области защиты информации;
- определять угрозы безопасности информации в информационных системах;
- формировать требования к обеспечению информационной безопасности данных при их обработке в информационных системах (формировать требования к системе защиты данных);

- выбирать организационные и технические меры, а также реализуемые ими мероприятия по обеспечению информационной безопасности данных при их обработке в информационных системах (разрабатывать систему защиты данных);

- внедрять способы и средства для обеспечения информационной безопасности данных при их обработке в информационных системах (внедрять систему защиты персональных данных);

- обеспечивать информационной безопасности данных в ходе эксплуатации информационных системах;

- обеспечивать информационной безопасности данных при выводе из эксплуатации информационных системах;

- устанавливать, настраивать, проводить техническое обслуживание программных (программно-аппаратных) средств защиты информации.

Целевая аудитория:

Руководители образовательной учреждений, заместители руководителей образовательных учреждений, специалисты, ответственные за обеспечение информационной безопасности.

Форма обучения: очная.

Срок освоения программы: 36 учебных часов.

Формы организации образовательного процесса: интерактивные лекции, практическая индивидуальная и групповая работа, работа в парах, выполнение заданий, подготовка методических материалов.

Программа реализуется: в группах по 25 человек с применением информационно-коммуникационной поддержки, в соответствии с графиком организации занятий.

Форма проведения итогового контроля: тестирование, выполнение практического задания (методической разработки).

УЧЕБНЫЙ ПЛАН

№ п/п	Наименование разделов и тем	Всего часов	Лекции	Практические занятия	Формы контроля
1.	Нормативно-правовая база информационной безопасности	3	2	1	Тест
2.	Анализ угроз информационной безопасности в образовательной среде	4	3	1	Памятка
3.	Средства и методы защиты информации	8	2	6	Памятка
4.	Организация информационной безопасности в образовательном учреждении	20	3	17	Локальные акты
5.	Педагогический практикум. Зачет	1	0	1	
		36	14	22	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование разделов и дисциплин	Всего часов	В том числе		Форма контроля/ аттестации
			Лекции	Практические занятия	
1	**Нормативно-правовая база**	**3**	**2**	**1**	

	информационной безопасности				
1.1	Федеральные законы РФ об информации, информационных технологиях и защите информации. Приказы Министерства просвещения РФ по вопросам информационной безопасности в образовательных организациях.	1	1		Тест
1.2	Локальные нормативные акты образовательной организации в сфере информационной безопасности	1	1	1	
2	**Анализ угроз информационной безопасности в образовательной среде**	**4**	**3**	**1**	
2.1	Классификация угроз информационной безопасности (внутренние и внешние, преднамеренные и случайные).	1	1		
2.2	Хакерские атаки, вредоносное ПО, социальная инженерия, фишинг, дипфейк.	2	1	1	Кейс
2.3	Утечки информации, их причины и последствия	1	1		
3	**Средства и методы защиты информации**	**8**	**2**	**6**	
3.1	Антивирусная защита, системы обнаружения вторжений, контент-фильтрация, электронно-цифровые подписи	2	1	1	Кейс
3.2	Сетевая безопасность: организация защищённой сети, межсетевые экраны, VPN.	1		1	Кейс
3.3	Защита данных: шифрование, резервное копирование	1		1	Кейс
3.4	Системы контроля доступа, аутентификация и авторизация, права доступа	2	1	1	Кейс
3.5	Безопасность поисковых запросов, безопасность облачных сервисов	1		1	Кейс
3.6	Защита локальных и беспроводных сетей	1		1	Кейс
4	**Организация информационной безопасности в образовательном учреждении**	**20**	**3**	**17**	
4.1.	Разработка политики информационной безопасности	2	1	1	

4.2	Разработка и исполнение локальных нормативных актов образовательной организации в сфере информационной безопасности	7	1	6	Локальные акты
4.3	Журналы по ведению деятельности в рамках информационной безопасности образовательной организации	2		2	Локальные акты
4.4	Обучение персонала основам информационной безопасности	1		1	Локальные акты
4.5	Безопасность в Интернете. Кибербуллинг.	1		1	Кейс
4.6	Профилактика игровой и интернетзависимости	1		1	Кейс
4.7	Проведение инвентаризации информационных ресурсов	1		1	Кейс
4.8	Использование разрешённого и рекомендуемого ПО в образовательной организации.	1		1	Кейс
4.9	Разработка планов реагирования на инциденты информационной безопасности	4	1	3	Локальные акты
5	**Педагогический практикум. Зачет**	**1**		**1**	

СОДЕРЖАНИЕ ПРОГРАММЫ

Тема 1. Нормативно-правовая база информационной безопасности.

(лекция – 2 ч., практическое занятие - 1 ч.)

Лекция.

Защищаемая информация и информационные ресурсы. Объекты информатизации. Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций. Организация работ по защите информации в информационных системах.

Основные понятия в области обеспечения безопасности персональных данных.

Обеспечение безопасности персональных данных при их обработке в информационных системах. Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.

Требования к защите персональных данных при их обработке в информационных системах.

Регуляторы в области обработки и обеспечения безопасности персональных данных, их задачи и распределение полномочий.

Система нормативных правовых актов по вопросам обеспечения безопасности персональных данных. Нормативные правовые акты ФСТЭК России и ФСБ России. Методические документы. Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации.

Организационно-правовые основы лицензирования деятельности по технической защите конфиденциальной информации.

Аттестация информационных систем, для которых их владельцами установлено требование по проведению оценки соответствия систем защиты информации на

соответствие требованиям по защите информации в государственных, региональных информационных системах.

Сертификация средств защиты информации по требованиям безопасности информации.

Ответственность за нарушение законодательства Российской Федерации в области персональных данных.

Практическая работа.

Разбор нормативно-правовой базы по организации безопасной образовательной среды.

Тема 2. Анализ угроз информационной безопасности в образовательной среде.

(лекция –3 ч., практическое занятие - 1 ч.)

Лекция.

Источники угроз безопасности информации. Классификационная схема угроз безопасности информации и их общая характеристика.

Угрозы целостности, конфиденциальности и доступности информации. Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах. Основные способы реализации угроз безопасности информации. Уязвимости информационных систем, используемые для реализации угроз безопасности информации. Методы определения актуальных угроз безопасности персональных данных в информационных системах.

Угрозы несанкционированного доступа. Характеристики угроз несанкционированного доступа к информации (воздействий на информацию) в информационных системах.

Защита информации при работе с системами управления базами данных.

Защита информации в локальных вычислительных сетях и при межсетевом взаимодействии. Характеристика типовых сетевых атак в информационных системах.

Методика оценки угроз безопасности информации, выявления уязвимостей в автоматизированных (информационных) системах.

Банк данных угроз безопасности информации, содержащий сведения об уязвимостях программного обеспечения, используемого в автоматизированных (информационных) системах.

Базы данных, содержащие описание уязвимостей информационных систем, в том числе CVE. Общая система оценки уязвимостей информационных систем (стандарты CVSS).

Модель угроз безопасности персональных данных в информационных системах. Порядок разработки модели угроз.

Состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных, с учетом актуальных угроз безопасности персональных данных в информационных системах.

Практическая работа.

Работа с кейсами реальных ситуаций информационных угроз. Разработка информационных плакатов. Разработка мониторингов по анализу информационной защищенности систем образовательной организаций и персональных данных.

Тема 3. Средства и методы защиты информации.

(лекция - 2 ч., практическое занятие - 6 ч.)

Лекция.

Цели и задачи системы защиты персональных данных и этапы ее жизненного цикла.

Требования к созданию систем защиты персональных данных и обеспечению их функционирования.

Требования к персоналу информационных системах.

Требования к организационно-распорядительным документам по обеспечению

безопасности персональных данных.

Требования к функционированию системы защиты персональных данных.

Мероприятия по созданию системы защиты персональных данных.

Стадии (этапы) работ по созданию систем защиты персональных данных (проектирование, разработка эксплуатационной документации, макетирование и тестирование системы защиты персональных данных информационных системах).

Установление требований к обеспечению безопасности персональных данных. Разработка проектной документации на информационных системах по защите персональных данных.

Выбор организационных и (или) технических мер, определенных с учетом актуальности угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

Разработка эксплуатационной, организационно-распорядительной документации на систему защиты персональных данных.

Тестирование функционирования систем защиты персональных данных и макетирование элементов системы.

Внедрение системы защиты персональных данных в информационных системах.

Предварительные испытания системы защиты персональных данных.

Опытная эксплуатация системы защиты персональных данных.

Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.

Обеспечение безопасности персональных данных в ходе эксплуатации информационных системах.

Обеспечение безопасности персональных данных при выводе из эксплуатации информационных системах или после принятия решения об окончании обработки персональных данных.

Виды и периодичность контроля за обеспечением уровня защищенности персональных данных, содержащихся в информационных системах, основные вопросы, подлежащие проверке.

Методы и средства контроля за обеспечением уровня защищенности персональных данных, содержащихся в информационных системах.

Порядок проведения контроля (анализа) защищенности персональных данных с учетом особенностей функционирования информационных системах.

Анализ и оценка функционирования информационных системах и ее системы защиты персональных данных, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты персональных данных.

Документирование процедур и результатов контроля за обеспечением уровня защищенности персональных данных, содержащейся в информационных системах.

Принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности персональных данных, о доработке (модернизации) системы защиты персональных данных.

Устранение недостатков по результатам контроля.

Практическая работа.

Работа с кейсами с правоприменительных практик по тематике. Разработка информационных памяток.

Тема 4. Организация информационной безопасности в образовательном учреждении.

(лекция - 3 ч., практическое занятие – 17 ч.)

Лекция.

Требования федерального государственного образовательного стандарта.

Информационная безопасность в образовательный учреждениях. Принципы информационной безопасности в образовательной среде. Угрозы информационной безопасности в образовательной среде. Виды средств защиты информации. Безопасность в Интернете. Кибербуллинг. Профилактика игровой и интернет-зависимости.

Практическая работа.

Работа с примерами локальных актов. Разбор кейсов (реальных проблемных ситуаций) в рамках заданной проблемы по организации информационной безопасности в образовательной среде.

Тема 5. Педагогический практикум. Зачет.

(практическое занятие - 1 ч.)

Практическая работа.

Представление итоговых разработок локальных актов (кейсов), выполненных на занятиях, с обсуждением в группах.

ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Контроль освоения материала

Занятия предполагают не только освоение информационного содержания курса, но и овладение методикой работы по созданию обеспечения условий информационной безопасности образовательной среды. Поэтому большое внимание уделяется организации самостоятельной работы слушателей.

В организации учебного процесса предусмотрены лекционные формы с применением интерактивных подходов. Таких как: вопрос-провокация, обмен мнениями по анализу текста, поиск дополнительной информации, ситуативное представление практик и опыта слушателей, вопросы-ответы групп слушателей, самостоятельная работа по изучению текста.

Итоговый контроль после завершения курса осуществляется по совокупности результатов всех видов контроля, предусмотренных программой.

Входной контроль

Форма: тестирование

Описание, требования к выполнению:

20 тестовых заданий, 20 мин. на выполнение.

Критерии оценивания:

Даны верные ответы на поставленный вопрос (1 балл за ответ). Высокий уровень - от 16 баллов Средний уровень - от 12 до 15 баллов Низкий уровень - до 11 баллов.

Примеры заданий:

1. Что такое информационная безопасность и какие ее основные компоненты вы знаете?
   а) Конфиденциальность, целостность, доступность
   б) Аутентификация, авторизация, учет
   в) Все вышеперечисленное
2. Какие основные угрозы информационной безопасности существуют в образовательных учреждениях?
   а) Вирусы и вредоносное ПО
   б) Хакерские атаки
   в) Социальная инженерия
   г) Несанкционированный доступ
3. Опишите основные принципы построения системы информационной безопасности.
   а) Минимизация атак
   б) Конфиденциальность, целостность, доступность
   в) Максимальное использование технологий
   г) Централизация управления

4. Какие нормативные документы регулируют вопросы информационной безопасности в образовательной сфере?

а) Федеральный закон "Об информации, информационных технологиях и о защите информации"

б) Приказы Министерства просвещения РФ

в) Локальные акты образовательной организации

г) Все вышеперечисленное

5. Что такое социальная инженерия и как защититься от нее?

а) Вид хакерской атаки, основанный на манипулировании людьми

б) Защита паролями и антивирусами

в) Обучение сотрудников правилам информационной безопасности

г) Все вышеперечисленное

6. Какое из следующих утверждений о политике информационной безопасности верно?

а) Это набор технических мер защиты информации

б) Это документ, определяющий правила и процедуры обеспечения безопасности информации

в) Это программное обеспечение для защиты информации

г) Это процесс обучения сотрудников

7. Что такое инцидент информационной безопасности?

а) Любое событие, которое может привести к нарушению конфиденциальности, целостности или доступности информации

б) Ошибка пользователя

в) Сбой оборудования

г) Плановое отключение системы

8. Какие меры необходимо принимать для предотвращения утечки информации?

а) Ограничение доступа к информации

б) Шифрование данных

в) Резервное копирование

г) Все вышеперечисленное

9. Какая из следующих мер не является эффективной для защиты от фишинга?

а) Использование антивирусного программного обеспечения

б) Проверка адреса отправителя электронного письма

в) Переход по ссылкам в подозрительных письмах

г) Ввод паролей на защищенных сайтах

10. Какая из следующих ролей не является ключевой в обеспечении информационной безопасности в образовательном учреждении?

а) Руководитель образовательного учреждения

б) Ответственный за информационную безопасность

в) Учитель информатики

г) Все сотрудники образовательного учреждения

Промежуточный контроль

Раздел программы:

Анализ угроз информационной безопасности в образовательной среде. Средства и методы защиты информации. Организация информационной безопасности в образовательном учреждении.

Форма:

Составление и решение ситуационных задач (кейсов)

Описание, требования к выполнению:

Промежуточный контроль проводится в форме составления и решения кейсов (реальных проблемных ситуаций). Промежуточный контроль предполагает выступление и

защиту своих позиций слушателем по составлению и решению кейсов в рамках заданной проблемы по организации безопасной образовательной среды. Возможно объединение слушателей в группы.

Критерии оценивания:

Критерии оценки:

1. В процессе составления кейса или выполнения проблемного задания в виде кейса было сформулировано и проанализировано большинство проблем в обозначенной области;

2. Были использованы дополнительные источники информации для составления или решения кейса;

3. Подготовленные в ходе составления или решения кейса материалы соответствуют требованиям к ним по смыслу и содержанию;

4.Выводы обоснованы, аргументы весомы;

5. Предложены оригинальные подходы к разработке кейса или сделаны креативные выводы, которые отличают данное решение кейса от других решений.

Показатели оценки:

По каждому критерию ставится 1-2 балла; максимум - 10 баллов; минимум - 5 баллов.

Оценка «отлично» - 9-10 баллов; оценка «хорошо» - 7-8 баллов; оценка «удовлетворительно» - 5-6 баллов.

Примеры заданий:

1. Предложите кейс работы с ребенком с девиантным поведением в Вашем образовательном учреждении;

2. Предложите кейс на основе работы с детьми с интернетзависимостью для Вашего образовательного учреждения;

3. Подготовьте кейс, направленный на осмысление проблемы создания безопасной образовательной среды, с учетом анализа всех компонентов образовательной среды вашей школы, ее модели;

4. Подготовьте кейс по проведению экспертизы безопасной образовательной среды вашей организации с учетом определения ее позитивных сторон и рисков.

5. Подготовьте кейс реализации простейшего генератора паролей, обладающего основными требованиями к парольным генераторам.

Количество попыток: не ограничено.

Промежуточный контроль

Раздел программы:

Организация информационной безопасности в образовательном учреждении.

Форма: Составление локальных актов

Описание, требования к выполнению:

Промежуточный контроль проводится в форме составления локальных актов образовательной организации по обеспечению информационное безопасности.

Критерии оценивания:

Критерии оценки:

1. Оформление локального акта;

2. Локальный акт учитывает особенности образовательной организации.

3. Выводы применения локального акта обоснованы;

4. Предложены оригинальные подходы к разработке локального акта, который решает проблематику обеспечения информационное безопасности образовательной организации.

Показатели оценки:

По каждому критерию ставится 1 балл; максимум - 4 баллов; минимум - 0 баллов.

Оценка «отлично» - 4 балла; оценка «хорошо» - 2-3 баллов; оценка «удовлетворительно» - 1 балл.

Примеры заданий:

1. Разработайте приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;

2. Разработайте приказ о назначении ответственного за обработку персональных данных в образовательном учреждении.

3. Разработайте приказ о создании комиссии по организации и проведению работ по защите персональных данных в образовательном учреждении.

4. Разработайте журнал учета передачи персональных данных.

5. Журнал учета прав доступа к материальным носителям персональных данных.

Количество попыток: не ограничено.

Итоговая аттестация

Итоговая аттестация осуществляется по совокупности результатов всех видов контроля, предусмотренных программой.

ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

Нормативные документы

Федеральные законы

1. Об образовании в Российской Федерации: Федеральный закон от 29.12.2012 № 273-ФЗ. URL: http://docs.cntd.ru/document/zakon-rf-ob-obrazovanii-v-rossijskoj-federacii (дата обращения 01.01.2024)
2. Об утверждении профессионального стандарта "Педагог (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель)»: приказ Минтруда Российской Федерации от 18.10.2013 № 544н URL: http://www.consultant.ru/document/cons doc LAW 155553/ (дата обращения 01.01.2024)
3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 № 149-ФЗ. URL: https://docs.cntd.ru/document/901990051?section=text (дата обращения 01.01.2024)
4. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 01.01.2024)
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». URL: https://docs.cntd.ru/document/901807667 (дата обращения 01.01.2024)
6. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». URL: https://docs.cntd.ru/document/901836556 (дата обращения 01.01.2024)
7. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400. URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения 01.01.2024)
8. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». URL: https://publication.pravo.gov.ru/Document/View/0001202205010023 (дата обращения 01.01.2024)
9. Положение о лицензировании деятельности по технической защите конфиденциальной информации. Утверждено постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79. URL: https://www.consultant.ru/document/cons_doc_LAW_125798/ (дата обращения 01.01.2024)
10. Требования к защите персональных данных при их обработке в

информационных системах персональных данных. Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119. URL: https://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения 01.01.2024)

11. Положение о банке данных угроз безопасности информации. Утверждено приказом ФСТЭК России от 16 февраля 2015 г. № 9. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения 01.01.2024)

12. Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 3 апреля 2018 г. № 55. URL: https://docs.cntd.ru/document/542622316 (дата обращения 01.01.2024)

13. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну. Утвержден приказом ФСТЭК России от 29 апреля 2021 г. № 77. URL: https://docs.cntd.ru/document/608228209 (дата обращения 01.01.2024)

14. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Утверждены приказом ФСТЭК России от 2 июня 2020 г. № 76. URL: https://docs.cntd.ru/document/566305930 (дата обращения 01.01.2024)

15. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. URL: https://docs.cntd.ru/document/499002630 (дата обращения 01.01.2024)

16. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21. URL: https://docs.cntd.ru/document/499005278 (дата обращения 01.01.2024)

17. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15 февраля 2008 г. URL: https://docs.cntd.ru/document/902330983 (дата обращения 01.01.2024)

18. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г. URL: https://docs.cntd.ru/document/607699443 (дата обращения 01.01.2024)

19. Методический документ. Методика тестирования обновлений безопасности программных, программно-аппаратных средств. Утвержден ФСТЭК России 28 октября 2022 г. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g (дата обращения 01.01.2024)

20. Методический документ. Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств. Утвержден ФСТЭК России 28 октября 2022 г. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-28-oktyabrya-2022-g-2 (дата обращения 01.01.2024)

21. Об утверждении методических указаний по осуществлению учета информационных систем и компонентов информационно-телекоммуникационной инфраструктуры. Приказ Министерства связи и массовых коммуникаций Российской Федерации от 31 мая 2013 г № 127. URL: https://docs.cntd.ru/document/499026861 (дата обращения 01.01.2024)

22. ГОСТ Р 2.610-2019 ЕСКД. Правила выполнения эксплуатационных документов. Ростехрегулирование, 2019. URL: https://docs.cntd.ru/document/1200164343 (дата обращения 01.01.2024)

23. ГОСТ 34.201-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем. Росстандарт,2021. URL: https://docs.cntd.ru/document/1200181803 (дата обращения 01.01.2024)
24. ГОСТ 34.602-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Росстандарт, 2021. URL: https://docs.cntd.ru/document/1200181804 (дата обращения 01.01.2024)
25. ГОСТ Р 59792-2021 Информационные технологии. Виды испытаний автоматизированных систем. Росстандарт, 2021. URL: https://docs.cntd.ru/document/1200181348 (дата обращения 01.01.2024)
26. ГОСТ Р 59793-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. Росстандарт, 2021. URL: https://docs.cntd.ru/document/1200181349 (дата обращения 01.01.2024)
27. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. URL: https://docs.cntd.ru/document/1200058320 (дата обращения 01.01.2024)
28. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. URL: https://docs.cntd.ru/document/1200108858 (дата обращения 01.01.2024)
29. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. URL: http://www.fa.ru/org/div/uank/Documents/2019/%D0%93%D0%9E%D0%A1%D0%A2%20%D0%A0%2051624-2000.pdf (дата обращения 01.01.2024)
30. ГОСТ Р 58412-2019 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения. Росстандарт, 2019. URL: https://docs.cntd.ru/document/1200164529 (дата обращения 01.01.2024)
31. ГОСТ Р ИСО/МЭК 27000-2021 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. Росстандарт, 2021. URL: https://docs.cntd.ru/document/1200179675 (дата обращения 01.01.2024)
32. ГОСТ Р ИСО/МЭК 27001-2021 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (на основе прямого применения международного стандарта ИСО/МЭК 27001:2005). Росстандарт, 2021. URL: https://docs.cntd.ru/document/1200181890 (дата обращения 01.01.2024)

Литература

1. Язов Ю.К. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Санкт-Петербург: Наукоемкие технологии, 2023. – 258 с.
2. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа. Монография / Ю.К. Язов, С.В. Соловьев – Воронеж: Кварта, 2018. – 588 с.
3. Баланов А.Н. Комплексная информационная безопасность: учебное пособие для СПО / А.Н. Баланов. – Санкт-Петербург: Лань, 2024. – 283 с.
4. Нестеров С.А. Основы информационной безопасности: учебник для вузов / С.А. Нестеров. – 3-е изд., стер. – Санкт-Петербург: Лань, 2024. – 324 с.
5. Прохоров О.В. Информационная безопасность и защита информации: учебник

для СПО / О.В. Прохоров. – 5-е изд., стер. – Санкт-Петербург: Лань, 2024. – 124 с.

6. Петренко В.И. Защита персональных данных в информационных системах. Практикум: учебное пособие для СПО / В.И. Петренко, И.В. Мандрица. – 2-е изд., стер. – Санкт-Петербург: Лань, 2022. – 108 с.

Электронные обучающие материалы

Электронные учебные материалы доступны в электронной информационно-образовательной среде ГБУ ДППО ЦПКС «Информационно-методический центр» Адмиралтейского района Санкт-Петербурга (доступно после регистрации на обучение).

Интернет-ресурсы

1. **Методические материалы по информационной безопасности на портале ГБУ ДПО «СПбЦОКОиИТ»** – https://docs.spbcokoit.ru
2. **Национальный форум информационной безопасности «ИНФОФОРУМ»**. Электронное периодическое издание по вопросам информационной безопасности (http://www.infoforum.ru/)
3. **Независимый** информационно-аналитический портал по безопасности - Anti-Malware.ru (http://www.anti-malware.ru/).
4. **Официальный интернет-портал правовой информации** – http://pravo.gov.ru/
5. **Консультант Плюс** – https://www.consultant.ru/
6. **Информационный правовой портал** – https://www.garant.ru/
7. **МВД России:**

https://мвд.рф/Videoarhiv/Socialnaja_reklama
https://мвд.рф/mvd/structure1/Upravlenija/убк
https://t.me/cyberpolice_rus

8. **Банк России:**

https://cbr.ru/protection_rights/finprosvet
https://vk.com/cbr_official
https://t.me/centralbank_Russia
https://dni-fg.ru/
https://fincult_info
https://doligra.ru
https://t.me/fintrack_cbr
https://t.me/fincult_info
https://vk.com/finprosv

9. **Минцифры России:**

https://www.gosuslugi.ru/cybersecurity
https://киберзож.рф/
https://выучисвоюроль.рф
https://прокачайскиллзащиты.рф
https://готовкцифре.рф
https://t.me/mintsifry

10. **Интернет – ресурсы финансово – кредитных учреждений, операторов связи и компаний, осуществляющих деятельность в сфере информационной безопасности**:

https://www.sberbank.ru/ru/person/kibrary
https://learn.vtb.ru/fingram/
https://megafon.ru/help/antifraud/
https://kaspersky.ru/resource-center
https://kids.kaspersky.ru/
https://rocit.ru

Материально-технические условия реализации программы. Технические средства обучения

Занятия по программе проводятся в современных аудиториях, оснащенных мультимедийной техникой и предназначенных для организации фронтальной, групповой и индивидуальной работы слушателей, в том числе в специально оборудованных компьютерных классах. Все слушатели обеспечиваются учебными материалами в электронной форме.