Министерство культуры Камчатского края
Краевое государственное бюджетное учреждение
дополнительного профессионального образования работников культуры
«Камчатский учебно-методический центр»
Отдел по повышению квалификации и
информационно-аналитической работе

СОГЛАСОВАНО:
Зав. отделом ПК
__ _____Е. А. Шевцова
«14» сентября 2021 г.

УТВЕРЖДАЮ:
Директор
_____Е.В. Галянт
«14» сентября 2021 г.

Дополнительная профессиональная образовательная программа повышения квалификации по направлению «Повышение квалификации специалистов по направлению “Информационные технологии»“»

по теме:

«Информационная безопасность бюджетных учреждений»
(Дистанционный семинар)

Петропавловск – Камчатский
2021

Содержание

1. Пояснительная записка.

Информационная безопасность (англ. Information Security, а также – англ. InfoSec) – практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача информационной безопасности – сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации. Это достигается, в основном, посредством многоэтапного процесса управления рисками, который позволяет идентифицировать основные средства и нематериальные активы, источники угроз, уязвимости, потенциальную степень воздействия и возможности управления рисками. Этот процесс сопровождается оценкой эффективности плана по управлению рисками.

Учебный курс разработан доцентом кафедры Библиотечно-информационной деятельности, документоведения и архивоведения Хабаровского Государственного Института Культуры (ХГИК) Киселёвым В.И.

2. Общие положения

2.1 Цель программы.

Целями освоения дисциплины является овладение теоретическими знаниями в области информационной безопасности.

2.2 Планируемые результаты освоения программы.

Повышение квалификации специалистов учреждений культуры направлено на совершенствование и актуализацию необходимых в их деятельности компетенций.

Процесс изучения курса направлен на формирование следующих компетенций: способность специалиста решать определенный класс профессиональных задач.

По завершении изучения курса слушатель должен:

Знать:

- Определения информационной безопасности;
- Технические методы и средства защиты информации.
- Программные методы защиты информации.

Уметь:

- Ориентироваться в законодательной базе по информационной безопасности;
- Своевременно отреагировать на нарушение в информационной безопасности и принять соответствующее решение.

2.3 Трудоемкость и срок освоения программы.

Трудоемкость программы в соответствии с календарным учебным графиком и учебным планом составляет 36 академических часов.

Виды учебных занятий: лекции. Режим проведения занятий – слушатель самостоятельно выбирает время для усвоения учебного материала.

Данная программа рассчитана на специалистов учреждений культуры, имеющих образование данного профиля, руководителей учреждений культуры.

2.4 Нормативные документы для разработки программы.

- Закон РФ «Об образовании» № 273-ФЗ от 29.12.2012 г.
- Приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

2.5 Категория слушателей и требования к уровню их подготовки.

Программа предназначена для специалистов учреждений культуры, имеющих специальное среднее/высшее образование.

2.6 Форма обучения.

Обучение заочное с применением ЭО.

2.7 Промежуточная и итоговая аттестация.

Формой итоговой аттестацией является выполнение практического задания.

По окончании курса будет выдано удостоверение государственного образца о повышении квалификации (Положение о порядке оформления, выдачи и хранения документов о дополнительном профессиональном образовании ОГУ от 03.12.2013 г. № 46-д).

3. Документы, регламентирующие содержание и организацию образовательного процесса при реализации программы.

3.1 Учебный план программы дистанционного семинара

№ п/п	Наименование модулей, разделов, тем	Объем работы слушателя, ч.				Формы контроля
		Всего	Аудиторная работа		Самостоятельная работа	
			ЛК	ПЗ/ЛЗ		
1	2	3	4	5	6	7
1.	Тема 1. Информационные ресурсы и их роль в обществе.	4	4	-	-	-
2.	Тема 2. Информационная безопасность.	4	4	-	-	-
3.	Тема 3. Угрозы информационной безопасности.	2	2	-	-	-
4.	Тема 4. Организационные методы защиты информации.	4	4	-	-	-
5.	Тема 5. Технические методы и средства защиты информации.	4	4	-	-	-
6.	Тема 6. Программные методы защиты информации.	2	2	-	-	-
7.	Тема 7. Компьютер-	6	6	-	-	-

	ная преступность и методы борьбы с ней.					
8.	Тема 8. Защита персональных данных.	4	4	-	-	-
9.	Тема 9. Обеспечение информационной безопасности в социально-культурной деятельности.	4	4	-	-	-
10.	Итоговая аттестация.	2	-	-	-	2
11.	**Всего:**	**36**	**34**	**-**	**-**	**2**

3.2 Примерный календарный учебный график.

Дистанционный семинар подразумевает работу слушателей в удобное для них время в течение срока обучения: 20 – 30 сентября 2021 года.

3.3 Рабочая программа учебных предметов, курсов, дисциплин (модулей).

Тема 1. Информационные ресурсы и их роль в обществе.

Понятие информационных ресурсов. Классификация информационных ресурсов. Документированные информационные ресурсы. Текстовые информационные ресурсы. Электронные информационные ресурсы. Информационные ресурсы и информационные услуги.

Тема 2. Информационная безопасность.

Проблема информационной безопасности. Информация как объект защиты. Сущность информации. Виды защищаемой информации. Источники и носители защищаемой информации.

Тема 3. Угрозы информационной безопасности.

Основные виды угроз информационной безопасности. Способы реализации угроз информационной безопасности. Основные принципы и методы защиты от угроз информационной безопасности.

Тема 4. Организационные методы защиты информации.

Правовое обеспечение защиты информации и информационной безопасности. Методы ограничения физического доступа к информационным объектам. Методы работы с персоналом.

Тема 5. Технические методы и средства защиты информации.

Технические средства поддержки ограничения физического доступа. Средства защиты акустической информации. Аппаратные средства обеспечения компьютерной безопасности.

Тема 6. Программные методы защиты информации.

Пароли и парольная защита информации. Контроль прав пользователей. Протоколирование и аудит в информационных сетях и системах. Средства и инструменты борьбы с компьютерными вирусами. Криптографические методы защиты информации.

Тема 7. Компьютерная преступность и методы борьбы с ней.

Понятие компьютерной преступности и виды компьютерных преступлений. Методы и средства борьбы с компьютерной преступностью.

Тема 8. Защита персональных данных.

Персональные данные и информационная безопасность личности. Правовые и программно-технические средства защиты персональных данных.

Тема 9. Обеспечение информационной безопасности в социально-культурной деятельности.

Особенности защиты информации в социально-культурной сфере. Организация системы обеспечения информационной безопасности.

Итоговая аттестация.

4. Учебно-методическое обеспечение

4.1 Рекомендуемая литература.

1. Аверченков В. И. Методы и средства инженерно-технической защиты информации : учеб. пособие / М.Ю. Рытов, А. В. Кувыклин, Т. Р. Гайнулин. – М.: ФЛИНТА, 2011. – 187 с. – (Серия «Организация и технология защиты информации»).
2. Башлы П. Н. Информационная безопасность : учебно-практическое пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – М. : Изд. центр ЕАОИ, 2010. – 376 с.
3. Блюмин А. М. Мировые информационные ресурсы : учебное пособие / А. М. Блюмин, Н.А. Феоктистов. – М. : Издательско-торговая корпорация «Дашков и К°», 2016. – 384 с.: ил. – (Учебные издания для бакалавров). – Библиогр. в кн.
4. Бузов Г. А. Защита от утечки информации по техническим каналам : Учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия – Телеком, 2005. – 416 с.
5. Варфоломеев А. А. Основы информационной безопасности : Учеб. пособие. – М. : РУДН, 2008. – 412 с.
6. Вехов В. Б. Компьютерные преступления. Способы совершения, методики расследования. – М. : Право и закон, 1996.
7. Гришина Н. В. Организация комплексной системы защиты информации. – М. : Гелиос АРВ, 2007. – 256 с.
8. Жук А. П. Защита информации : Учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин и др. – М. : РИОР: ИНФРА-М, 2015. – 392 с.

9. Иванов А. В. Защита речевой информации от утечки по акустоэлектрическим каналам : учебное пособие / А.В. Иванов, В. А. Трушин. – Новосибирск : НГТУ, 2012. – 43 с. : ил. табл., схем.
10. Киселев В.И. Информационная безопасность и защита информации : Учебное пособие. – Хабаровск : ХГИК, 2018. – 122 с.
11. Лапонина О. Р. Криптографические основы безопасности. – М. : Национальный Открытый Университет «ИНТУИТ», 2016. – 244 с. : ил. – (Основы информационных технологий).
12. Скрипник, Д. А. Обеспечение безопасности персональных данных : курс / Д. А. Скрипник ; Национальный Открытый Университет "ИНТУИТ". – М.: Интернет-Университет Информационных Технологий, 2011. – 109 с. : ил. , схем.
13. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 31.12.2017).
14. Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".
15. Фабричнов А.Г. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / А. Г. Фабричнов, А. С. Дёмушкин, Т. В. Кондрашова, Н. Н. Куняев. – М. : Логос, 2011. – 452 с. - (Новая университетская библиотека).
16. ФЗ «Об информации, информационных технологиях и защите информации» №149-ФЗ от 27.07.2006.
17. ФЗ «О персональных данных» №152-ФЗ от 27.07.2006 с изменениями от 27.12.2009 (ФЗ №363).

17.1 Информационные средства обеспечения дисциплины.

1. //biblioclub.ru/index.php?page=book&id=453024
2. //biblioclub.ru/index.php?page=book&id=228846
3. //biblioclub.ru/index.php?page=book&id=429092

4. //biblioclub.ru/index.php?page=book&id=235577
5. //biblioclub.ru/index.php?page=book&id=234794
6. //www.consultant.ru/document/cons_doc_LAW_10699/
7. //biblioclub.ru/index.php?page=book&id=84996
8.

4.3 Материально-техническое обеспечение курса.

Для прохождения курса повышения квалификации (семинара) необходим выход в Internet, персональный компьютер (планшет).

5. Фонд оценочных средств.

Итоговый зачёт.

Тест для итогового контроля знаний (зачёт)

Тест содержит 15 вопросов, рассчитан на 45 минут, вариант правильного ответа на каждый вопрос только один.

Критерий оценивания результатов прохождения теста:
не удовлетворительно – правильно выполнено 8 и менее заданий,
удовлетворительно – 9-11 правильно выполненных заданий,
хорошо – 12-13 правильно выполненных заданий,
отлично – 14-15 правильно выполненных заданий.

Задание № 1. Что такое конфиденциальность информации?

а) Свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации;

б) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);

в) Свойство информации, заключающееся в ее существовании в виде не защищенного паролем набора;

г) Свойство информации, заключающееся в ее шифровании.

Задание № 2. Что не относится к угрозам информационной безопасности?

а) **Классификация информации по видам;**

б) Событие, действие, процесс или явления, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному её тиражированию;

в) Стихийные бедствия (наводнения, ураган, землетрясение, пожар);

г) Сбои и отказы оборудования (технических средств) автоматизированных систем;

д) Ошибки эксплуатации (пользователей, операторов и другого персонала);

е) Преднамеренные действия нарушителей и злоумышленников.

Задание № 3. Что относится к правовым мерам защиты информации?

а) Законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения;

б) Действия правоохранительных органов для защиты информационных ресурсов;

в) Организационно-административные меры для защиты информационных ресурсов;

г) Действия администраторов сети для защиты информационных ресурсов.

Задание № 4. Что такое государственная тайна?

а) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ;

б) Сведения о состоянии окружающей среды;

в) Все сведения, которые хранятся в государственных базах данных;

г) Сведения о состоянии здоровья президента РФ.

Задание № 5. Что такое коммерческая тайна?

а) Информация, имеющая действительную или потенциальную коммерческую ценность в силу её неизвестности третьим лицам;

б) Информация, содержащая в учредительных документах;

в) Информация, содержащая в годовых отчетах, бухгалтерских балансах, формах государственных статистических отчетов.

Задание № 6. Что такое несанкционированный доступ (НСД)?

а) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;

б) Создание резервных копий в организации;

в) Правила и положения, выработанные в организации для обхода парольной защиты;

г) Удаление ненужной информации.

Задание № 7. Что такое идентификация?

а) Процесс распознавания элемента системы, обычно с помощью заранее определённого идентификатора или другой уникальной информации;

б) Указание на правильность выполненных операций по защите информации;

в) Определение файлов, которые изменены в информационной системе несанкционированно;

г) Выполнение процедуры засекречивания файлов;

д) Процесс периодического копирования информации.

Задание № 8. Что такое электронная цифровая подпись?

а) Реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный с использованием закрытого ключа и позволяющий идентифицировать владельца подписи, а также установить отсутствие искажения информации в документе;

б) Набор цифр персонально закрепленных за пользователями, неразрешенных к использованию любыми другими пользователями;

в) Индивидуальный код, известный ограниченному кругу пользователей и зашифрованный симметричным ключом.

Задание № 9. Выберите правильный вариант ответа.

Какой вид информации не требует защиты:

а) Государственная тайна;

б) Врачебная тайна;

в) Коммерческая тайна;

г) Информация о погоде.

Задание № 10. Вставьте пропущенное понятие.

В криптографических механизмах защиты используется секретный …

а) Ключ;

б) Носитель;

в) Агент.

Задание № 11. Какое из направлений защиты информации не относится к программным средствам?

а) Экранирование компьютерной техники;

б) Архивирование файлов;

в) Шифрование файлов.

Задание № 12. Какой из способов задания паролей является наиболее надежным?

а) Произвольная комбинация цифр и букв в нижнем и верхнем регистре;

б) Дата рождения пользователя;

в) Имя одного из членов семьи пользователя;

г) Название любимой книги (фильма, музыкального исполнителя);

д) Нецензурное выражение.

Задание № 13. Для какого из способов защиты целесообразно применять

программы-архиваторы файлов?

а) Резервного копирования файлов на съемные носители;

б) Санкционирования доступа к устройствам и данным;

в) Шифрование конфиденциальной информации.

Задание № 14. Процесс преобразования открытых данных в закрытые для защиты от несанкционированного использования (чтения, распространения) называется:

а) Дешифрование;

б) Регистрация;

в) Шифрование;

г) Аутентификация;

д) Секьюритизация.

Задание № 15. "Специально написанная, обычно небольшая по размерам программа, которая размножается путем записи своих копий в другие программы и в системные области дисков, производящая нежелательные действия". Это определение:

а) Компьютерного драйвера;

б) Компьютерного вируса;

в) Компьютерной оболочки;

г) Компьютерного змея.

№ задания	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Правильный ответ	а	а	а	а	а	а	а	а	г	а	а	а	а	в	б

6. Форма контроля.

Контроль успеваемости обучающихся – важнейшая форма контроля образовательной деятельности, включающая в себя целенаправленный систематический мониторинг освоения обучающимися примерной программы повышения квалификации в целях:

- получения необходимой информации о выполнении обучающимися дополнительной профессиональной программы повышения квалификации;
- оценки уровня знаний, умений и приобретенных (усовершенствованных) обучающимися компетенций;
- стимулирования самостоятельной работы обучающихся.

Итоговая аттестация (квалификационный экзамен) для обучающихся проводится в соответствии с требованиями, установленными Федеральным законом от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», приказом Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

Освоение примерной дополнительной профессиональной программы повышения квалификации завершается итоговой аттестацией в форме выполнения практического задания.

7. Входные требования к слушателям.

Слушатели данных курсов должны иметь высшее или средне-специальное образование.

Также слушатели должны уметь обращаться с компьютером на уровне не ниже среднего.

8. Выходные требования к слушателям.

К итоговой аттестации допускаются лица, выполнившие требования, предусмотренные курсом обучения по программе

повышения квалификации и успешно прошедшие все промежуточные аттестационные испытания, предусмотренные учебным планом.

Итоговая аттестация проводится в сроки, предусмотренные учебным планом и календарным графиком учебного процесса.

Слушатель признается «успешно освоившим курс» при выполнении всех заданий. По окончании обучения он получает удостоверение государственного образца.

Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации оценку «неудовлетворительно», а также лицам, освоившим часть примерной программы повышения квалификации, удостоверение не выдается.

РАЗРАБОТЧИК ПРОГРАММЫ:

_____ _____

(должность) (Ф.И.О, подпись)

СОГЛАСОВАНО:

_____ _____

(должность) (Ф.И.О, подпись)