МИНИСТЕРСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ
И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СИБИРСКАЯ ПОЖАРНО-СПАСАТЕЛЬНАЯ АКАДЕМИЯ» ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ»

УТВЕРЖДАЮ
Заместитель начальника ФГБОУ ВО
Сибирская пожарно-спасательная
академия ГПС МЧС России
по учебной работе
полковник внутренней службы
М.В. Елфимова
«26» марта 2020 г.

РАБОЧАЯ ПРОГРАММА
учебной дисциплины
Б1.В.24 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
направление подготовки 38.03.04 Государственное
и муниципальное управление
профиль Управление в кризисных ситуациях
квалификация бакалавр

Железногорск
2020

1. Цели и задачи дисциплины «Информационная безопасность»

Цели освоения дисциплины «Информационная безопасность»:

– формирование системы знаний об основах защиты информации в локальной и глобальной сети и основах защиты баз данных;

– формирование представлений об основных векторах программных, криптографических и социально-инженерных атак; эффективных методах и приемах информационной защиты;

Задачи дисциплины «Информационная безопасность»:

– овладение приемами и стандартными практиками защиты информации;

– формирование эффективных навыков информационной защиты личной, служебной и ведомственной информации;

– формирование умений по использованию базовых программных средств и практик защиты личных, служебных и ведомственных информационных ресурсов;

– изучение номенклатуры технологических решений, служебных протоколов и имеющихся методов информационной защиты.

2. Перечень планируемых результатов обучения по дисциплине «Информационная безопасность», соотнесенных с планируемыми результатами освоения образовательной программы

Изучение дисциплины «Информационная безопасность» направлено на формирование у обучающихся компетенций, представленных в таблице.

Содержание компетенции	Код компетенции	Результаты обучения
1	2	3
способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-6	Знает основные векторы программных, криптографических и социально-инженерных атак; основные методы и приемы информационной защиты.
		Умеет использовать средства и приемы информационной защиты.
		Владеет навыками организации безопасного создания, хранения и передачи информации с учетом основных требований информационной безопасности.
способностью осуществлять технологическое обеспечение служебной деятельности специалистов (по категориям и группам должностей государственной гражданской службы и муниципальной службы)	ПК-16	Знает нормативную базу, методы и типовые технологические протоколы и программные средства информационной защиты.
		Умеет применять типовые программные средства для организации защиты личной, служебной и ведомственной информации.
		Владеет навыками защиты информации и технологического обеспечения служебной деятельности специалистов (по категориям и группам должностей государственной гражданской службы и муниципальной службы).

3. Место дисциплины «Информационная безопасность» в структуре образовательной программы

Учебная дисциплина «Информационная безопасность» относится к вариативной части Блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы высшего образования по направлению подготовки 38.03.04 Государственное и муниципальное управление (уровень бакалавриата) профиль «Управление в кризисных ситуациях».

4. Объем дисциплины «Информационная безопасность» в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных единицы (108 часов).

для заочной формы обучения (4 года 6 месяцев)

Вид учебной работы, формы контроля	**Всего часов**	**Курс**
		2
Общая трудоемкость дисциплины в часах	**108**	**108**
Общая трудоемкость дисциплины в зачетных единицах	**3**	**3**
Контактная работа с обучающимися	**10**	**10**
в том числе:		
Лекции	4	4
Практические занятия	6	6
Лабораторные работы		
Самостоятельная работа	**94**	**94**
Вид аттестации	зачет (4)	зачет (4)

5. **Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий**

5.1. Разделы учебной дисциплины «Информационная безопасность» и виды занятий

Заочная форма обучения

№ п.п.	Наименование разделов и тем	Всего часов	Количество часов по видам занятий			Промежуточная аттестация	Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы		
1	2	3	4	5	6	7	8
2 курс							
1	Основы информационной безопасности	44	2				42
2	Векторы информационных атак	34	2	4			28
3	Приемы и методы информационной защиты	26		2			24
	Зачет	**4**				**4**	
	Итого за 2 курс	**108**	**4**	**6**		**4**	**94**
	Итого по дисциплине	**108**	**4**	**6**		**4**	**94**

5.2. Содержание учебной дисциплины «Информационная безопасность»

Тема 1. Основы информационной безопасности

Лекция:

1. История информационной безопасности.
2. Государственная политика Российской Федерации в области информационной безопасности.
3. Нормативные основы информационной безопасности.

Самостоятельная работа:

1. Нормативные положения, касающиеся информационной безопасности.
2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации.
3. Основы единой технической политики МЧС России в области информационных технологий и информационной безопасности.

Рекомендуемая литература:

Основная [1, 2].

Дополнительная [1, 3].

Тема 2. Векторы информационных атак

Лекция:

1. Криптографические методы получения незаконного доступа.
2. Программно-технические методы.
3. Социально-инженерные методы.

Практическое занятие «Основные виды несанкционированного доступа»:

1. Атаки, использующие вставки скриптов в интерпретируемые среды.
2. Атаки «подмены источника».
3. Атаки «отказа в обслуживании».
4. Эксплуатация режима исполнения «исполнение вне очереди».

Самостоятельная работа:

1. Социально-инжиниринговые атаки.
2. Криптографические атаки.
3. Атаки, использующие уязвимости программных средств.
4. Сетевые атаки.
5. Атаки, использующие уязвимости операционных систем.

Рекомендуемая литература:

Основная [1, 2].

Дополнительная [2].

Тема 3. Приемы и методы информационной защиты

Практическое занятие «Приемы и методы информационной защиты»:

1. Просмотр и удаление метаинформации в электронных документах.
2. Программные средства шифрования.

Самостоятельная работа:

1. Профилактика социально-инжиниринговых атак.
2. Профилактика криптографические атак.
3. Профилактика сетевых атак.
4. Профилактика атак, использующих уязвимости программных средств.

Рекомендуемая литература:

Основная [1, 2].

Дополнительная [1, 3].

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине «Информационная безопасность»

Для обеспечения самостоятельной работы обучающихся по дисциплине используется учебно-методическое и информационное обеспечение, указанное в разделе 8 настоящей программы, а также методические рекомендации по организации самостоятельной работы, разрабатываемые кафедрой.

Для выполнения контрольной работы обучающимися по заочной форме кафедрой разрабатываются методические рекомендации по ее выполнению.

7. Оценочные средства для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине «Информационная безопасность»

Оценочные средства дисциплины «Информационная безопасность» включают в себя следующие разделы:

1. Типовые контрольные вопросы для оценки знаний, умений, навыков, характеризующих формирование компетенций в процессе освоения дисциплины.
2. Методику оценивания персональных образовательных достижений обучающихся.

7.1. Типовые контрольные задания или иные материалы для оценки знаний, умений и навыков, характеризующих формирование компетенций в процессе освоения дисциплины

7.1.1. Текущий контроль

Текущий контроль осуществляется в соответствии с материалами, разрабатываемыми кафедрой, включающими: тесты, контрольные вопросы по темам дисциплины, задания для выполнения контрольной работы. В ходе изучения дисциплины обучающийся по заочной форме выполняет 1 контрольную работу.

7.1.2. Промежуточная аттестация

Примерный перечень вопросов к зачету

1. Закон об информации, информационных технологиях и о защите информации.
2. Закон о безопасности критической информационной инфраструктуры Российской Федерации.
3. Закон о связи и информационная безопасность.
4. Виды и функции электронной подписи.
5. Защита персональных данных.
6. Основы единой технической политики МЧС России.
7. Опасности «закладок» и импортозамещение.
8. Социально-инжиниринговые атаки, их виды.
9. Примеры социально-инжиниринговых атак.
10. Фишинг и целевой фишинг.
11. Сетевые атаки.
12. Программы-прослушиватели сетевых протоколов.
13. Сканирование сетевых портов.
14. Сетевые сканеры.
15. Регистрация и аудит системы.
16. Атаки на сетевую инфраструктуру.

17. Атаки вида «отказ в обслуживании».
18. Атаки, использующие уязвимости программных средств.
19. Уязвимость «переполнение стека».
20. VPN-соединения.
21. Атаки, использующие скриптовые вставки в интерпретирующие программные среды.
22. Атака SQL-insertion.
23. «Санация» пользовательского ввода.
24. Атака «подмены источника».
25. Криптографические атаки.
26. Классические шифры: шифр Цезаря, Виженера, Кардано.
27. Шифровальные блокноты.
28. Устаревшие и актуальные шифры. DES-шифрование.
29. Понятие «односторонней» функции.
30. Симметричные системы шифрования.
31. Асимметричные системы шифрования.
32. Электронная цифровая подпись.
33. Хэш-функции.
34. Управление криптографическими ключами.
35. Стеганографические методы шифрования данных.
36. Атаки, использующие словари паролей.
37. Атаки, использующие уязвимости операционных систем.
38. Уязвимости Meltdown и Spectre.
39. Профилактика социально-инжиниринговых атак.
40. Профилактика криптографических атак.
41. Профилактика атак, использующих уязвимости программных сред.
42. Профилактика атак на сетевую инфраструктуру.
43. Профилактика атак на операционные системы.
44. Прямые и косвенные признаки программно-вирусного заражения.
45. Виды вирусных атак.
46. Вирусы «трояны».
47. Запись с клавиатуры (key-logging).
48. Вирусы шифровальщики.
49. Профилактика программно-вирусных заражений.
50. Нетрадиционные методы несанкционированного доступа.
51. Организация доступа в современных операционных системах.
52. Обеспечение безопасности операционных систем.
53. Задачи системного администрирования.
54. Управление политикой безопасности.
55. Разграничение доступа.
56. Изоляция программ.
57. Изоляция среды исполнения.
58. Виртуализация операционных систем.
59. Виртуальные среды исполнения (контейнеры).

7.2. Методика оценивания персональных образовательных достижений обучающихся

Промежуточная аттестация: зачёт

Достигнутые результаты освоения дисциплины	Критерии оценивания	Шкала оценивания
Обучающийся имеет существенные пробелы в знаниях основного учебного материала по дисциплине; не способен аргументированно и последовательно его излагать, допускает грубые ошибки в ответах, неправильно отвечает на задаваемые вопросы или затрудняется с ответом.	Не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание большей или наиболее важной части учебного материала; допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов.	«Не зачтено»
Обучающийся освоил знания, умения, компетенции и теоретический материал без пробелов; выполнил все задания, предусмотренные учебным планом; правильно, аргументировано ответил на все вопросы, с приведением примеров; при ответе продемонстрировал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов.	Продемонстрировано умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер; в изложении допущены небольшие пробелы, не исказившие содержание ответа; допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя.	«Зачтено»

8. Требования к условиям реализации. Ресурсное обеспечение дисциплины «Информационная безопасность»

8.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины «Информационная безопасность»

Основная:

1. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – Москва: РИОР, 2013. – 222 с. Текст: электронный. – URL: https://znanium.com/catalog/product/405000. – Режим доступа: по подписке.
2. Информационная безопасность: практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. – Самара: Самарский юридический институт ФСИН России, 2019. – 84 с. Текст: электронный. – URL: https://znanium.com/catalog/product/1094244. – Режим доступа: по подписке.

Дополнительная:

1. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – 4-е изд., перераб. и доп. – Москва: РИОР: ИНФРА-М, 2021. – 336 с. (Высшее образование). Текст: электронный. – URL: https://znanium.com/catalog/product/1189326. – Режим доступа: по подписке.
2. Моторыгин Ю.Д. Информационная безопасность: лабораторный практикум [Текст] / Ю.Д. Моторыгин, В.А. Ловчиков, Ю.Г. Паринова – СПб.: Санкт-Петербургский университет ГПС МЧС России ГПС МЧС России, 2013. – 54 с.
3. Сычев, Ю. Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. – Москва: ИНФРА-М, 2021. – 201 с. – (Высшее образование: Бакалавриат). – Текст: электронный. – URL: https://znanium.com/catalog/product/1013711. – Режим доступа: по подписке.

8.2. Перечень программного обеспечения, используемого при осуществлении образовательного процесса

1. Операционная система Calculate Linux Desktop Пакет офисных программ Libre Office
2. Антивирусная защита – Kaspersky Endpoint Security для Linux
3. Браузер Mozilla Firefox
4. Программа просмотра электронных документов в формате PDF Adobe Acrobat Reader DC
5. Архиватор 7zip

8.3. Перечень информационно-справочных систем и баз данных

1. Центральная ведомственная электронная библиотека МЧС России – ELIB.MCHS.RU (ip-адрес: 10.46.0.45).
2. Электронная библиотечная система «Знаниум» (URL: www.znanium.com).
3. Электронные научные журналы и базы данных Сибирского федерального университета (URL: libproxy.bik.sfu-kras.ru).
4. Электронно-библиотечная система «ЮРАЙТ». Раздел «Легендарные Книги» (URL: www.biblio-online.ru).
5. Национальная электронная библиотека «НЭБ» (URL: https://нэб.рф).
6. Информационная система «Единое окно» (URL: window.edu.ru).
7. Международный научно-образовательный сайт EqWorld (URL: eqworld.ipmnet.ru/indexr.htm).
8. Электронная библиотека научных публикаций eLIBRARY.RU (URL: https://elibrary.ru/).
9. Информационно-правовая система «Консультант плюс» (URL: http://www.consultant.ru/).
10. Информационно-правовая система «Гарант» (URL: https://www.garant.ru/).
11. Электронная информационно-образовательная среда ФГБОУ ВО Сибирская пожарно-спасательная академия (URL: https://sibpsa.ru/personal/personal.php).

8.4. Материально-техническое обеспечение дисциплины «Информационная безопасность»

Для материально-технического обеспечения дисциплины «Информационная безопасность» необходимы учебные аудитории для проведения занятий лекционного типа, семинарского типа, текущего контроля и промежуточной аттестации. Помещение должно быть укомплектовано специализированной мебелью и техническими средствами обучения (компьютером, мультимедийным проектором, экраном), служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Академии.

9. Методические указания по освоению дисциплины «Информационная безопасность»

Программой дисциплины «Информационная безопасность» предусмотрены занятия лекционного типа, занятия семинарского типа и самостоятельная работа обучающихся.

Цели лекционных занятий:

- дать систематизированные научные знания по дисциплине, акцентировав внимание на наиболее сложных вопросах дисциплины;
- стимулирование активной познавательной деятельности обучающихся, способствование формированию их творческого мышления.

Цели практических занятий:

- углубление и закрепление знаний, полученных на лекциях и в процессе самостоятельной работы обучающихся с учебной и научной литературой;
- овладение практическими умениями и навыками профессиональной деятельности;
- развитие абстрактного и логического мышления.

Цели самостоятельной работы обучающихся:

- углубление и закрепление знаний, полученных на лекциях и других занятиях;
- выработка навыков самостоятельного активного приобретения новых, дополнительных знаний;
- подготовка к предстоящим учебным занятиям и промежуточному контролю.

При реализации различных видов учебных занятий для наиболее эффективного освоения дисциплины «Информационная безопасность» используются следующие образовательные технологии:

1. Технология контекстного обучения – обучение в контексте профессии, реализуется в учебных заданиях, учитывающих специфику направления и профиля подготовки; применяется при проведении занятий лекционного типа, семинарского типа, самостоятельной работе.
2. Технология интерактивного обучения – реализуется в форме учебных заданий, предполагающих взаимодействие обучающихся, использование активных форм обратной связи; применяется при проведении занятий семинарского типа.
3. Технология электронного обучения – реализуется при выполнении учебных заданий с использованием электронной информационно-образовательной среды Академии, информационно-справочных и поисковых систем, проведении автоматизированного тестирования и т.д.; применяется при проведении занятий семинарского типа, самостоятельной работе.

9.1. Рекомендации для преподавателей

Лекция является главным звеном дидактического цикла обучения. Ее цель – формирование ориентировочной основы для последующего усвоения обучающимися учебного материала. В ходе лекции преподаватель, применяя методы устного изложения и показа, передает обучающимся знания по основным, фундаментальным вопросам дисциплины «Информационная безопасность».

Назначение лекции состоит в том, чтобы доходчиво, убедительно и доказательно раскрыть основные теоретические положения изучаемой науки, нацелить обучающихся на наиболее важные вопросы, темы, разделы дисциплины, дать им установку и оказать помощь в овладении научной методологией (методами, способами, приемами) получения необходимых знаний и применения их на практике.

К лекции как к виду учебных занятий предъявляются следующие основные требования:

- научность, логическая последовательность изложения учебных вопросов;
- конкретность и целеустремленность изложения материала;
- соответствие отводимого времени значимости учебных вопросов;
- соответствие содержания лекции принципам обучения, требованиям руководящих документов;
- наглядность обучения; формирование у обучаемых потребности к самостоятельному углублению знаний;
- изложение материала с учетом достигнутого уровня знаний.

При подготовке и проведении занятий семинарского типа преподавателю, ведущему дисциплину, в первую очередь необходимо опираться на настоящую рабочую программу, в которой определены количество и тематика лабораторных работ и практических занятий.

Для каждого занятия определяются тема, цель, структура и содержание. Исходя из них, выбираются форма проведения занятия (комбинированная, самостоятельная работа, фронтальный опрос, тестирование и т.д.) и дидактические методы, которые при этом применяет преподаватель (индивидуальная работа, работа по группам, деловая игра и пр.).

Современные требования к преподаванию обуславливают использование визуальных и аудиовизуальных технических средств представления информации: презентаций, учебных фильмов и т.д.

Для обеспечения самостоятельной работы обучающихся по дисциплине преподавателем разрабатываются методические рекомендации по организации самостоятельной работы.

При разработке заданий для самостоятельной работы необходимо выполнять следующие требования:

- отбор и изложение материала должны обеспечивать достижение целей, изложенных в квалификационной характеристике, и понимание прикладного значения данного курса для своей профессии;

- материал заданий должен быть методологичен, осознаваем и служить средством выработки обобщенных умений;
- при составлении заданий следует формулировать их содержание в контексте специальности.

Для успешного выполнения контрольной работы обучающимися по заочной форме преподавателем разрабатываются методические рекомендации по ее выполнению.

9.2. Рекомендации для обучающихся

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других видах занятий, выработку навыков самостоятельного приобретения новых, дополнительных знаний, подготовку к предстоящим учебным занятиям и промежуточной аттестации.

Основными видами самостоятельной работы являются: работа с печатными источниками информации (конспектом, книгой, документами), информационно-справочными системами и базами данных (раздел 8 настоящей программы).

Вопросы, отнесенные на самостоятельное изучение (раздел 5 настоящей программы), даются преподавателем в ходе лекций и (или) занятий семинарского типа. При этом обучающемуся необходимо уяснить и записать вопросы, посмотреть рекомендованную литературу и наметить общую структуру изучения вопроса в виде плана или схемы. Затем изучить информацию по вопросу, при этом рекомендуется вести конспект, куда вносится ключевая информация, формулы, рисунки. Перечитать сделанные в конспекте записи. Убедиться в ясности изложенного, при необходимости дополнить записи.

В ходе лекций и (или) занятий семинарского типа обучающийся ведет конспект кратко, схематично, последовательно с фиксированием основных положений, выводами, формулировками, обобщениями, помечает важные мысли, выделяет ключевые слова, термины. Для закрепления знаний после занятия рекомендуется перечитать материал и записать вопросы, которые не ясны из прочитанного. По этим вопросам необходимо обратится к учебной литературе и, если в результате работы с учебной литературой остались вопросы – следует обратиться за разъяснениями к преподавателю в часы консультаций.

При подготовке к практическим занятиям обучающемуся необходимо изучить основную литературу, ознакомиться с дополнительной литературой, учесть рекомендации преподавателя.

Самостоятельная работа обучающегося по заочной форме включает выполнение одной контрольной работы.

Рабочая программа учебной дисциплины разработана в соответствии с ФГОС ВО по направлению подготовки 38.03.04 Государственное и муниципальное управление (уровень бакалавриата).

УТВЕРЖДЕНО
Протокол заседания кафедры физики, математики
и информационных технологий

№_____ от_____

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе *(модуле)* дисциплины_____
(название дисциплины)
по направлению подготовки *(специальности)*_____
на 20__/20__ учебный год

1. В _____ вносятся следующие изменения:
(элемент рабочей программы)
1.1. ……..;
1.2. ……...;
…
1.9. …… .

2. В _____ вносятся следующие изменения:
(элемент рабочей программы)
2.1. ……..;
2.2. ……...;
…
2.9. …… .

3. В _____ вносятся следующие изменения:
(элемент рабочей программы)
3.1. ……..;
3.2. ……...;
…
3.9. …… .

Составитель подпись расшифровка подписи
дата