МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
"Казанский (Приволжский) федеральный университет"
Институт фундаментальной медицины и биологии

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Таюрский Д.А.
_____
"___"_____20___ г.

Программа дисциплины

Основы информационной безопасности Б1.В.ДВ.16

Направление подготовки: 44.03.05 - Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Образование в области физической культуры и безопасности жизнедеятельности
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Салихов Н.Р.

Рецензент(ы):

Галеев И.Ш.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Мустаев Р. Ш.
Протокол заседания кафедры No ___ от "____" _____ 201__г

Учебно-методическая комиссия Института фундаментальной медицины и биологии:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Салихов Н.Р. кафедра безопасности жизнедеятельности и общей физической подготовки Центр биологии и педагогического образования , NRSalihov@kpfu.ru

1. Цели освоения дисциплины

Повышение компьютерной грамотности в вопросах защиты информации от несанкционированного доступа.

Задачи курса:

1. Ознакомить с государственной и корпоративной политикой в области охраны информации и авторских прав
2. Изучить основные средства и методы защиты информации
3. Рассмотреть негативные факторы информации

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел "Б3+.ДВ.4 Цикл профессиональных дисциплин и относится к базовой (общепрофессиональной) части". Осваивается на втором курсе.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК - 2 (общекультурные компетенции)	способностью анализировать основные этапы и закономерности исторического развития для формирования патриотизма и гражданской позиции
ОК - 3 (общекультурные компетенции)	способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве
ОК - 5 (общекультурные компетенции)	способностью работать в команде, толерантно воспринимать социальные, культурные и личностные различия
ОК - 7 (общекультурные компетенции)	способностью использовать базовые правовые знания в различных сферах деятельности
ОК - 9 (общекультурные компетенции)	способностью использовать приемы первой помощи, методы защиты в условиях чрезвычайных ситуаций
ОПК-2 (профессиональные компетенции)	способностью осуществлять обучение, воспитание и развитие с учетом социальных, возрастных, психофизических и индивидуальных особенностей, в том числе особых образовательных потребностей обучающихся
ПК-8 (профессиональные компетенции)	способностью проектировать образовательные программы

В результате освоения дисциплины студент:

1. должен знать:

- юридическую основу защиты информации

 негативные факторы информации

2. должен уметь:

Применять основные аппаратные и программные средства защиты информации.

3. должен владеть:

информационной безопасностью.

4. должен демонстрировать способность и готовность:

к применению полученных знаний и навыков на практике и в своей профессиональной деятельности.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 9 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Понятие информационная безопасность.	9	1-3	2	0	0	Устный опрос
2.	Тема 2. Государственная политика в обеспечении информационной безопасности.	9	4-6	4	2	0	Устный опрос
3.	Тема 3. Корпоративная политика в области защиты информации и авторских прав.	9	7-9	2	2	0	Дискуссия
4.	Тема 4. Методы и средства обеспечения безопасности информации.	9	10-12	4	2	0	Письменное домашнее задание
5.	Тема 5. Негативное воздействие информации.	9	13-15	2	2	0	Устный опрос
.	Тема . Итоговая форма контроля	9		0	0	0	Зачет
	Итого			14	8	0	

4.2 Содержание дисциплины

Тема 1. Понятие информационная безопасность.

лекционное занятие (2 часа(ов)):

Признаки информационной эпохи Понятие "информация" и "информационная безопасность" и их содержание. Формирование показателей информационной безопасности

Тема 2. Государственная политика в обеспечении информационной безопасности.

лекционное занятие (4 часа(ов)):

Основы государственной политики обеспечения информационной безопасности. Законодательство в области информационной безопасности.

практическое занятие (2 часа(ов)):

1. Конституция Российской Федерации, законодательство Российской Федерации, общепризнанные принципы и нормы международного права по обеспечению информационной безопасности Российской Федерации; 2. Открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации; 3. Правовое равенство всех участников процесса информационного 4. Право граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом; 5. Приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Тема 3. Корпоративная политика в области защиты информации и авторских прав.

лекционное занятие (2 часа(ов)):

Основы защиты деловой информации и сведений, составляющих служебную, коммерческую, государственную тайну. Защита интеллектуальной собственности.

практическое занятие (2 часа(ов)):

1. Государственная тайна. Понятие и его содержание. 2. Органы государственной власти и должностные лица, определяющие перечень сведений, составляющих государственную тайну. 3. Перечень сведений, составляющих государственную тайну: - Сведения в военной области ; - Сведения в области экономики, науки и техники; - Сведения в области внешней политики и экономики, преждевременное распространение которых может нанести ущерб безопасности государства; - Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности. 4. Органы защиты государственной тайны. 5. Коммерческая тайна. Понятие и его содержание. 6. Право на отнесение информации к составляющей коммерческую тайну и способы получения такой информации. 7. Сведения, которые не могут составлять коммерческую тайну.

Тема 4. Методы и средства обеспечения безопасности информации.

лекционное занятие (4 часа(ов)):

Основные факторы и ключевые проблемы информационной безопасности. Аппаратные средства обеспечения приватности информации. Программное обеспечение профилактики несанкционированного доступа к информации.

практическое занятие (2 часа(ов)):

1. Методы и средства обеспечения безопасности информации: препятствие, маскировка, регламентация, принуждение и побуждение. 2. Формальные средства защиты: технические средства, аппаратные устройства, физические, устройства и системы и программные средства. 3. Неформальные средства защиты: организационные средства, морально-этические средства и законодательные средства.

Тема 5. Негативное воздействие информации.

лекционное занятие (2 часа(ов)):

Информационные технологии и здоровье. Негативные последствия глобальной информатизации и рекламы, их дестабилизирующее воздействие на человека.

практическое занятие (2 часа(ов)):

1. Определение объекта защиты, т.е. что именно защищается от негативного информационно-психологического воздействия (руководство структуры, органы управления, коммуникационные линии, персонал, члены семей сотрудников). 2. Определение потенциальной угрозы, т.е. какому воздействию оказывать противодействие. Кто противник и какое негативное информационно-психологическое воздействие, на каком уровне может осуществляться. Насколько это информационное воздействие является негативным с точки зрения влияния на выполнение функциональных задач. 3. Выявление каналов возможного негативного информационно-психологического воздействия (СМИ, листовки, письма, телефонные контакты, SMS-сообщения и т.д.). 4. Определить возможный ущерб или степень того, что именно необходимо предотвратить, чего нужно избежать (уничтожения, разрушения, расчленения, подчинения, формирования неверных установок). 5. Определение пути и средства противодействия, т.е. определить то, как избежать возможного ущерба, каким образом противодействовать в зависимости как от специфики и возможностей объекта защиты, так и от характеристик опасности, наличия сил и средств у субъектов противодействия. 6. Определить субъект противодействия (руководство, органы управления, общественные организации, сотрудники).

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Понятие информационная безопасность.	9	1-3	подготовка к контрольной работе	8	контрольная работа
2.	Тема 2. Государственная политика в обеспечении информационной безопасности.	9	4-6	подготовка к контрольной работе	12	контрольная работа
3.	Тема 3. Корпоративная политика в области защиты информации и авторских прав.	9	7-9	подготовка к контрольной работе	10	контрольная работа
4.	Тема 4. Методы и средства обеспечения безопасности информации.	9	10-12	подготовка к контрольной работе	12	контрольная работа
5.	Тема 5. Негативное воздействие информации.	9	13-15	подготовка к контрольной работе	8	контрольная работа
	Итого				50	

5. Образовательные технологии, включая интерактивные формы обучения

Освоение дисциплины "Информационная безопасность" предполагает использование как традиционных (лекции, практические занятия с использованием методических материалов), так и инновационных образовательных технологий с использованием в учебном процессе активных и интерактивных форм проведения занятий: выполнение ряда практических заданий с использованием профессиональных программных средств создания и ведения электронных баз данных; мультимедийных программ, включающих подготовку и выступления студентов на семинарских занятиях с фото-, аудио- и видеоматериалами по предложенной тематике.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Понятие информационная безопасность.

контрольная работа , примерные вопросы:

Примерные вопросы: 1. Признаки информационной эпохи 2. Что такое информационная безопасность 3. Формирование показателей информационной безопасности

Тема 2. Государственная политика в обеспечении информационной безопасности.

контрольная работа , примерные вопросы:

Примерные вопросы: 1. Проблемы региональной информационной безопасности 2. Нормативно-правовые акты в сфере обеспечения информационной безопасности

Тема 3. Корпоративная политика в области защиты информации и авторских прав.

контрольная работа , примерные вопросы:

Примерные вопросы: 1. Методы нарушения конфиденциальности информации 2. Методы нарушения доступности и целостности информации 3. Причины, виды, каналы утечки искажения информации. 4. Интеллектуальная собственность и авторское право

Тема 4. Методы и средства обеспечения безопасности информации.

контрольная работа , примерные вопросы:

Примерные вопросы: 1. Политика безопасности 2. Модель нарушителя 3. Организационные меры 4. Технические средства защиты информации.

Тема 5. Негативное воздействие информации.

контрольная работа , примерные вопросы:

Примерные вопросы: 1. Психофизиологические негативные факторы применения информационных и коммуникационных технологий. 2. Негативное воздействие электромагнитного излучения аппаратных средств информационных технологий. 3. Информационная война.

Итоговая форма контроля

зачет (в 9 семестре)

Примерные вопросы к итоговой форме контроля

Пример вопросов к зачету:

1. Признаки информационной эпохи
2. Что такое информационная безопасность
3. Формирование показателей информационной безопасности
4. Проблемы региональной информационной безопасности
5. Нормативно-правовые акты в сфере обеспечения информационной безопасности
6. Методы нарушения конфиденциальности информации
7. Методы нарушения доступности и целостности информации
8. Причины, виды, каналы утечки искажения информации.
9. Интеллектуальная собственность и авторское право

10. Политика безопасности
11. Модель нарушителя
12. Организационные меры по защите информации
13. Технические средства защиты информации.
14. Психофизиологические негативные факторы применения информационных и коммуникационных технологий.
15. Негативное воздействие электромагнитного излучения аппаратных средств информационных технологий.
16. Информационная война.

7.1. Основная литература:

1. Расторгуев, Сергей Павлович. Основы информационной безопасности: учебное пособие для студентов высших учебных заведений / С.П. Расторгуев.?Москва: Академия, 2007. - 186 с.

2. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.- ISBN 978-5-91134-627-0 http://znanium.com/bookread.php?book=420047

3. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. - ISBN 978-5-8199-0331-5. http://znanium.com/bookread.php?book=335362

4. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. http://znanium.com/bookread.php?book=405000

7.2. Дополнительная литература:

1. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-91134-360-6. http://znanium.com/bookread.php?book=405313

2. Максим М., Безопасность беспроводных сетей [Электронный ресурс] / Мерритт Максим, Дэвид Поллино ; Пер. с англ. Семенова А. В. - М. : ДМК Пресс, 2008. - 288 с. (Информационные технологии для инженеров.) - ISBN 5-94074-248-3 - Режим доступа: http://www.studentlibrary.ru/book/ISBN5940742483.html

3. Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс] / Н. Н. Куняев. - М.: Логос, 2010. - 348 с. - ISBN 978-5-98704-513-8.http://znanium.com/bookread.php?book=469026

4. Региональная и национальная безопасность: Учебное пособие / А.Б. Логунов. - М.: Вузовский учебник, 2009. - 432 с.: 60x90 1/16. (переплет) ISBN 978-5-9558-0093-6. http://znanium.com/bookread.php?book=153774

7.3. Интернет-ресурсы:

StudFiles. Все для учебы. - http://www.studfiles.ru/

Безопасность. Образование. Человек. - http://www.bezopasnost.edu66.ru/

Гало - http://www.galo.ru/

Е.С. Бажанова. Основы безопасности жизнедеятельности. Учебное пособие - http://www.bestreferat.ru/

Журнал ОБЖ Основы безопасности жизни - http://www.russmag.ru/

Министерство по делам гражданской обороны и чрезвычайным ситуациям Республики Татарстан - http://mchs.tatarstan.ru/

МЧС России - http://www.mchs.gov.ru/

Научно-практический и учебно-методический журнал Безопасность жизнедеятельности. - http://www.novtex.ru/

Образовательные ресурсы Интернета - Безопасность жизнедеятельности. - http://www.alleng.ru/

Спас экстрим. Портал детской безопасности МЧС России. - http://www.zarnitza.ru/

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Основы информационной безопасности" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "КнигаФонд", доступ к которой предоставлен студентам. Электронно-библиотечная система "КнигаФонд" реализует легальное хранение, распространение и защиту цифрового контента учебно-методической литературы для вузов с условием обязательного соблюдения авторских и смежных прав. КнигаФонд обеспечивает широкий законный доступ к необходимым для образовательного процесса изданиям с использованием инновационных технологий и соответствует всем требованиям новых ФГОС ВПО.

1.Лекционная аудитория с мультимедиапроектором, ноутбуком и экраном на штативе.

2. Аудитории для практических занятий.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 44.03.05 "Педагогическое образование (с двумя профилями подготовки)" и профилю подготовки Образование в области физической культуры и безопасности жизнедеятельности .

Автор(ы):
Салихов Н.Р. _____
"__" _____ 201 __ г.

Рецензент(ы):
Галеев И.Ш. _____
"__" _____ 201 __ г.