МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Шуйский филиал ИвГУ

Кафедра безопасности жизнедеятельности и адаптивной физической культуры

ОДОБРЕНО:

Руководитель ОП
_____ А.Б. Гогин
(подпись)

«29» июня 2023 г.

Рабочая программа дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования:	бакалавриат
Квалификация выпускника:	бакалавр
Направление подготовки:	44.03.05 Педагогическое образование (с двумя профилями подготовки)
Направленность (профиль) образовательной программы:	Физическая культура; Безопасность жизнедеятельности

Шуя

1. Цели освоения дисциплины

– формирование у студентов систематизированных знаний о принципах и средствах обеспечения информационной безопасности личности, конкретных объектов и учреждений, общества и государства.

2. Место дисциплины в структуре ОП

Дисциплина «Информационная безопасность» является обязательной для изучения; относится к обязательной части блока дисциплин Б1; входит в предметно-методический модуль.

Успешное освоение данной дисциплины будет способствовать готовности обучающихся к освоению дисциплин: безопасность жизнедеятельности; обеспечение комплексной безопасности учащихся и воспитанников; прохождению учебной практики, технологической (проектно-технологической) практики, по предметно-методическому модулю; учебной практики, ознакомительной практики, по предметно-методическому модулю; производственной практики, технологической (проектно-технологической) практики, по предметно-методическому модулю; учебной практики, научно-исследовательской работы (получение первичных навыков научно-исследовательской работы), по предметно-методическому модулю; дистанционные технологии в образовательном процессе школы; мультимедиа технологии в образовании; прохождению государственной итоговой аттестации.

Студент, приступающий к изучению данной дисциплины, должен:

Знать:

– особенности системного и критического мышления;

– основы современных технологий сбора, обработки и представления информации;

– современные угрозы, опасности и риски в киберпространстве;

– превентивные мероприятия по обеспечению безопасности в образовательной организации;

– научные основы преподаваемого предмета, его историю и место в мировой культуре и науке (конкретизируются применительно к изучаемой учебной дисциплине);

– этапы развития предметной области;

– содержательные, методологические и мировоззренческие связи предметной области со смежными научными областями.

Уметь:

– анализировать источники информации с точки зрения временных и пространственных условий их возникновения;

– получать, обрабатывать и анализировать информацию из различных источников;

– анализировать ранее сложившиеся в науке оценки информации;

– аргументированно формировать собственное суждение и оценку информации;

– выстраивать алгоритм безопасного поведения в киберпространстве;

– применять различные методы защиты в опасных и чрезвычайных ситуациях;

– совершенствовать свои профессиональные знания и умения на основе постоянного самообразования;

– руководствоваться в профессиональной деятельности научными основами преподаваемого предмета (конкретизируются применительно к изучаемой учебной дисциплине);

– соотносить основные этапы развития предметной области с ее актуальными задачами, методами и концептуальными подходами, тенденциями и перспективами ее современного развития;

– устанавливать содержательные, методологические и мировоззренческие связи предметной области со смежными научными областями.

Владеть:

– навыками сопоставления разных источников информации с целью выявления их противоречий и поиска достоверных суждений;

– навыками определения практических последствий предложенного решения задач;

– технологиями анализа и синтеза информации на основе системного подхода;

– приемами организации безопасной и комфортной образовательной среды;

– способами совершенствования профессиональных знаний и умений путем использования информационной среды.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

3.1. Компетенции, формированию которых способствует данная дисциплина

При реализации дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

а) универсальные компетенции (УК) и индикаторы их достижения:

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Код и наименование индикатора достижения универсальной компетенции
Системное и критическое мышление	УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Демонстрирует знание особенностей системного и критического мышления и готовность к нему. УК-1.2. Применяет логические формы и процедуры, способен к рефлексии по поводу собственной и чужой мыслительной деятельности. УК-1.3. Анализирует источник информации с точки зрения временных и пространственных условий его возникновения. УК-1.4. Анализирует ранее сложившиеся в науке оценки информации. УК-1.5. Сопоставляет разные источники информации с целью выявления их противоречий и поиска достоверных суждений. УК-1.6. Аргументировано формирует собственное суждение и оценку информации, принимает обоснованное решение. УК-1.7. Определяет практические последствия предложенного решения задачи.

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции выпускника	Код и наименование индикатора достижения универсальной компетенции
Безопасность жизнедеятельности	УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.	УК.8.1. Оценивает факторы риска, умеет обеспечивать личную безопасность и безопасность окружающих в повседневной жизни и в профессиональной деятельности, а также при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов. УК.8.2. Формирует культуру безопасного и ответственного поведения в повседневной жизни и в профессиональной деятельности, а также использует методы защиты в чрезвычайных ситуациях и военных конфликтах.

б) общепрофессиональные компетенции (ОПК) и индикаторы их достижения:

Наименование категории (группы) общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции выпускника	Код и наименование индикатора достижения общепрофессиональной компетенции
Научные основы педагогической деятельности	ОПК-8. Способен осуществлять педагогическую деятельность на основе специальных научных знаний	ОПК-8.1. Применяет методы анализа педагогической ситуации, профессиональной рефлексии на основе специальных научных знаний. ОПК-8.2. Проектирует и осуществляет учебно-воспитательный процесс с опорой на знания основных закономерностей возрастного развития когнитивной и личностной сфер обучающихся, научно-обоснованных закономерностей организации образовательного процесса, научных основ преподаваемых предметов, их истории и места в мировой культуре и науке. ОПК-8.3. Осуществляет мониторинг и отбор программ профессионального и личностного развития.

3.2. Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения формируемых компетенций

В результате освоения дисциплины обучающийся должен:

Знать:

– особенности системного и критического мышления (УК-1 (индикаторы – 1, 2, 3, 4, 5, 6, 7));

– основы современных технологий сбора, обработки и представления информации (УК-1 (индикаторы – 1, 2, 3, 4, 5, 6, 7));

– основные опасности, угрозы, характер их воздействия на человека, общество и окружающую среду (УК-8 (индикаторы – 1, 2));

– современные угрозы, опасности и риски в киберпространстве (УК-8 (индикаторы – 1, 2));

– правила безопасного поведения и методы защиты от опасных и чрезвычайных ситуаций в процессе жизнедеятельности (УК-8 (индикаторы – 1, 2));

– превентивные мероприятия по обеспечению безопасности в образовательной организации (УК-8 (индикаторы – 1, 2));

– научные основы преподаваемого предмета, его историю и место в мировой культуре и науке (конкретизируются применительно к изучаемой учебной дисциплине) (ОПК-8 (индикаторы – 1, 2, 3));

– этапы развития предметной области (ОПК-8 (индикаторы – 1, 2, 3));

– содержательные, методологические и мировоззренческие связи предметной области со смежными научными областями (ОПК-8 (индикаторы – 1, 2, 3)).

Уметь:

– анализировать источники информации с точки зрения временных и пространственных условий их возникновения (УК-1 (индикаторы – 1, 2, 3, 4, 5, 6, 7));

– получать, обрабатывать и анализировать информацию из различных источников (УК-1 (индикаторы – 1, 2, 3, 4, 5, 6, 7));

– анализировать ранее сложившиеся в науке оценки информации (УК-1 (индикаторы – 1, 2, 3, 4, 5, 6, 7));

– аргументированно формировать собственное суждение и оценку информации (УК-1 (индикаторы – 1, 2, 3, 4, 5, 6, 7));

– оценивать факторы риска и выстраивать алгоритм безопасного поведения в условиях чрезвычайных ситуаций и военных конфликтов (УК-8 (индикаторы – 1, 2));

– выстраивать алгоритм безопасного поведения в киберпространстве (УК-8 (индикаторы – 1, 2));

– применять различные методы защиты в опасных, чрезвычайных ситуациях и военных конфликтах (УК-8 (индикаторы – 1, 2));

– формировать у детей и подростков мотивацию к здоровому образу жизни и культуру безопасного поведения (УК-8 (индикаторы – 1, 2));

– использовать здоровьесберегающие технологии в организации образовательного пространства (УК-8 (индикаторы – 1, 2));

– организовывать и проводить работу с учащимися, родителями (законными представителями) обучающихся и персоналом образовательных организаций по формированию навыков безопасного поведения при возникновении опасных и чрезвычайных ситуаций (УК-8 (индикаторы – 1, 2));

– проводить профилактические мероприятия по предупреждению детского травматизма (УК-8 (индикаторы – 1, 2));

– совершенствовать свои профессиональные знания и умения на основе постоянного самообразования (ОПК-8 (индикаторы – 1, 2, 3));

– руководствоваться в профессиональной деятельности научными основами преподаваемого предмета (конкретизируются применительно к изучаемой учебной дисциплине) (ОПК-8 (индикаторы – 1, 2, 3));

– соотносить основные этапы развития предметной области с ее актуальными задачами, методами и концептуальными подходами, тенденциями и перспективами ее современного развития (ОПК-8 (индикаторы – 1, 2, 3));

– устанавливать содержательные, методологические и мировоззренческие связи предметной области со смежными научными областями (ОПК-8 (индикаторы – 1, 2, 3)).

Владеть:

– навыками сопоставления разных источников информации с целью выявления их противоречий и поиска достоверных суждений (УК-1 (индикаторы – 1, 2, 3, 4, 5, 6, 7));

– навыками определения практических последствий предложенного решения задач (УК-1 (индикаторы – 1, 2, 3, 4, 5, 6, 7));

– технологиями анализа и синтеза информации на основе системного подхода (УК-1 (индикаторы – 1, 2, 3, 4, 5, 6, 7)).

– методами формирования культуры безопасного и ответственного поведения в повседневной жизни и в профессиональной деятельности (УК-8 (индикаторы – 1, 2));

– приемами и технологиями проведения мероприятий по сохранению природной среды и обеспечению устойчивого развития общества (УК-8 (индикаторы – 1, 2));

– способами совершенствования профессиональных знаний и умений путем использования информационной среды (ОПК-8 (индикаторы – 1, 2, 3)).

4. Объём и содержание дисциплины

Очная форма обучения

Объём дисциплины составляет 3 зачётные единицы (81 час.)
Контактная работа 25,83 час.
Самостоятельная работа 55,17 час.

Виды учебных занятий и формы промежуточной аттестации	1 сем.	
	Контактная работа с преподавателем	Самостоятельная работа обучающегося
Лекции	12	30
Практические занятия	12	
Групповые консультации перед экзаменом	1,5	-
Экзамен	0,33	25,17
Всего 81	25,83	55,17

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и объемом учебных занятий

Очная форма обучения

№ п/п	Раздел (тема) дисциплины	Семестр	Виды учебных занятий, включая самостоятельную работу обучающихся и объем (в часах)				Формы текущего контроля успеваемости Формы промежуточной аттестации
			Занятия лекционного типа	Занятия семинарского типа		Самостоятельная работа обучающегося	
				Лаб.	Пр.		
1.	Проблемы и угрозы информационной безопасности	1	3		3	6	
2.	Основы государственной политики обеспечения информационной безопасности	1	3		3	6	
3.	Основные направления обеспечения информационной безопасности	1	3		3	6	Текущий контроль 1
4.	Сущность и методы дестабилизирующего информационного воздействия на человека	1	1,5		1,5	6	
5.	«Глобальное общество» и проблемы информационной безопасности	1	1,5		1,5	6	Текущий контроль 2
ИТОГО			**12**		**12**	**30**	**Экзамен**

4.2. Развернутое описание содержания учебного материала по разделам (темам)

Тема 1. Проблемы и угрозы информационной безопасности.

Понятие информационной безопасности. Основные проблемы информационной безопасности и пути их решения. Виды и источники угроз информационной безопасности. Информационные противостояния от древности до Нового времени. Информационные войны XX века. Место информационной безопасности в системе национальной безопасности России.

Тема 2. Основы государственной политики обеспечения информационной безопасности.

Конституция РФ и Доктрина информационной безопасности РФ о правовом обеспечении информационной сферы. Федеральное законодательство в сфере информационной безопасности. Указы Президента РФ и иные нормативно-правовые акты по вопросам информационной безопасности. Организационное обеспечение информационной безопасности. Международное сотрудничество России в области обеспечения информационной безопасности.

Тема 3. Основные направления обеспечения информационной безопасности.

Основы защиты деловой информации и сведений, составляющих служебную, коммерческую, государственную тайну. Защита информации в экономике, внутренней и внешней политике, науке и технике. Защита интеллектуальной собственности. Информационное обеспечение оборонных мероприятий и боевых действий. Понятие информационной войны. Обеспечение информационной безопасности в правоохранительной сфере и при возникновении чрезвычайных ситуаций. Методы и средства защиты электронной информации. Безопасность в сфере духовной жизни человека и общества.

Тема 4. Сущность и методы дестабилизирующего информационного воздействия на человека.

Сущность и современное состояние манипуляции сознанием и поведением людей. Основные методы и средства информационного воздействия на человека. Мифы как инструмент воздействия на людей. Манипулятивные технологии в избирательных кампаниях. Технологии «черного пиара». Дестабилизирующее влияние слухов. Влияние средств массовой информации на мировоззрение людей и духовно-нравственное становление подрастающих поколений. Роль рекламы в манипуляции сознанием людей. Повседневно-бытовой уровень манипуляции сознанием. Средства информационного воздействия и защита здоровья.

Тема 5. «Глобальное общество» и проблемы информационной безопасности.

Объективные и субъективные предпосылки создания глобального общества. Роль Интернета в мировом информационном пространстве. Глобальные ожидания и опасения человечества. Негативные последствия глобальной информатизации общества.

5. Образовательные технологии, в том числе перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

В процессе изучения дисциплины предусматривается использование следующих образовательных технологий, методов обучения и инновационных форм учебных занятий: технологии проблемного обучения, технологий развития критического мышления, технологии коллективного способа обучения, рейтинговой технологии, интерактивных занятий.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: мультимедиа технологии; технологии визуализации (инфографика, скрайбинг, презентационная графика); интерактивные информационные технологии; технологии Веб 2.0.

Для подготовки докладов, выполнения индивидуальных заданий студенты используют электронный каталог библиотеки, электронные ресурсы электронных библиотечных систем «Университетская книга» (Режим доступа: www.biblioclub.ru), ЭБС Шуйского филиала ИвГУ на платформе «Руконт».

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся по дисциплине осуществляется в следующих формах:

1) выполнение контрольных работ;
2) изучение разделов программы с целью подготовки к промежуточной аттестации;
3) подготовка домашних практических работ, индивидуальных сообщений по избранной теме.

Полностью весь методический материал по обеспечению самостоятельной работы студентов приводится в приложении 1 к настоящей программе. Доступ к методическим материалам осуществляется через сайт Шуйского филиала ИвГУ, в том числе через ЭБС Шуйского филиала ИвГУ на платформе «Руконт».

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине

Для текущего контроля успеваемости используются такие виды работ, как тесты, кейс-задачи и контрольная работа, которые выполняются самостоятельно.

На экзамене по дисциплине «Информационная безопасность» контролируемые знания, умения и владения, характеризующие этапы формирования компетенций в процессе освоения образовательной программы, проверяются разноуровневыми заданиями: тест-задание (пороговый уровень), контрольная работа (базовый уровень) и кейс-задачи (повышенный уровень).

На экзамене используется письменная форма проведения экзамена, а также рейтинговая (накопительная) система оценивания результатов обучения. Задания контрольной работы выполняются в процессе самостоятельной работы по подготовке к экзамену. Максимальное количество баллов, которое можно получить на экзамене – 30 баллов.

Тестирование проводится на зачёте в течение 40 минут. Каждый вариант тест-билета содержит 20 заданий в тестовой форме.

Критерии оценки:

Каждое правильно выполненное задание оценивается 0,5 балла, максимальное количество баллов – 10.

Если по отдельной теме студент набирает количество баллов ниже зачётного, то тема считается неосвоенной и баллы в рейтинг не прибавляются.

Контрольная работа выполняется письменно в процессе самостоятельной работы по подготовке к экзамену. Свой вариант задания студент получает за 10 дней до экзамена. Задание проверяется и оценивается на экзамене.

Критерии оценки:

Задание оценивается в 15 баллов. При оценивании учитываются следующие критерии:

Критерии формирования оценки	Шкала оценивания
1. Точность разработки самостоятельного задания. 2. Логичность и системность построения самостоятельного задания. 3. Владение терминологическим аппаратом. 4. Умение привести примеры, иллюстрирующие теоретические положения. 5. Грамотно, аккуратно выполнена практическая часть.	12-15 баллов
1. Информация с фактической стороны представлена верно. 2. Работа выстроена системно, в логической последовательности. 3. Термины используются корректно, и их значение объясняется студентом. 4. Приводятся примеры на теоретические положения. 5. Грамотно, аккуратно выполнена практическая часть самостоятельной работы, но с небольшими отклонениями.	8-11 баллов
1. Информация с фактической стороны представлена верно. 2. Допущены нарушения принципа системности в построении работы. 3. Допущена неточная трактовка некоторых терминов. 4. Имеются затруднения с нахождением примеров	4-7 баллов

подтверждения теоретического положения. 5. Грамотно, но неаккуратно выполнена практическая часть самостоятельной работы.	
1. Информация с фактической стороны представлена не совсем верно. 2. Работа выстроена с нарушением логической последовательности. 3. Студент некорректно трактует базовые термины. 4. Студент не может привести примеры, иллюстрирующие теоретические положения. 5. Не выполнена практическая часть контрольной работы.	1-3 балла

Кейс-задачи выполняются студентом письменно на экзамене.

Критерии оценки:

Задание оценивается в 5 баллов. При оценивании учитываются следующие критерии:

Критерии формирования оценки	Шкала оценивания
1. изложение материала логично, грамотно, без ошибок; 2. свободное владение профессиональной терминологией; 3. умение высказывать и обосновать свои суждения; 4. студент дает четкий, полный, правильный ответ на теоретические вопросы; 5. студент организует связь теории с практикой.	4-5 баллов
1. студент грамотно излагает материал; ориентируется в материале, владеет профессиональной терминологией, осознанно применяет теоретические знания для решения кейса, но содержание и форма ответа имеют отдельные неточности; 2. ответ правильный, полный, с незначительными неточностями или недостаточно полный.	3 балла
1. студент излагает материал неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения кейса, не может доказательно обосновать свои суждения; 2. обнаруживается недостаточно глубокое понимание изученного материала	2 балла
1. отсутствуют необходимые теоретические знания; допущены ошибки в определении понятий, искажен их смысл, не решен кейс; 2. в ответе студента проявляется незнание основного материала учебной программы, допускаются грубые ошибки в изложении, не может применять знания для решения кейса.	1 балл

Оценка результатов освоения дисциплины при рейтинговой системе оценивания формируется по 100-балльной шкале из результатов текущего контроля успеваемости и

результатов, полученных на экзамене.

Оценка на экзамене выставляется по следующей шкале:

Шкала оценки результатов освоения дисциплины «Информационная безопасность» при рейтинговой системе оценивания

Повышенный уровень	Базовый уровень	Пороговый уровень	Ниже порогового уровня
5 (отлично)	4 (хорошо)	3 (удовлетворительно)	2 (неудовлетворительно)
85-100 баллов	71-84 балла	61-70 баллов	60 и менее баллов

Фонд оценочных средств по дисциплине «Информационная безопасность» в полном объёме представлен в Приложении 2 к рабочей программе.

8. Учебно-методическое и информационное обеспечение дисциплины

Учебная и учебно-методическая литература:

– основная литература:

1. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. – Орел : Межрегиональная академия безопасности и выживания, 2014. – 257 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428605. – Текст : электронный.
2. Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=362895. – ISBN 978-5-4475-3947-4. – DOI 10.23681/362895. – Текст : электронный.
3. Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562348. – ISBN 978-5-238-02857-6. – Текст : электронный.

– дополнительная литература:

1. Башлы, П. Н. Информационная безопасность: учебно-практическое пособие : учебное пособие / П. Н. Башлы, Е. К. Баранова, А. В. Бабаш. – Москва : Евразийский открытый институт, 2011. – 375 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=90539. – ISBN 978-5-374-00301-7. – Текст : электронный.
2. Ефимова, Л. Л. Информационная безопасность детей: российский и зарубежный опыт / Л. Л. Ефимова, С. А. Кочерга. – Москва : Юнити-Дана, 2017. – 240 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=682995. – ISBN 978-5-238-02405-9. – Текст : электронный.
3. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 255 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=276557. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный.

4. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.
5. Основы национальной безопасности : учебное пособие для студентов высших учебных заведений / Л. А. Михайлов [и др.]. - Москва : Академия, 2008. - 176 с.
6. Петров, С. В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.
7. Расторгуев, С.П. Основы информационной безопасности : учебное пособие для студентов высших учебных заведений / С. П. Расторгуев. - Москва : Академия, 2007. - 192 с.
8. Сычев, Ю. Н. Основы информационной безопасности : учебно-практическое пособие : учебное пособие / Ю. Н. Сычев. – Москва : Евразийский открытый институт, 2010. – 328 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=90790. – ISBN 978-5-374-00381-9. – Текст : электронный.

Интернет-ресурсы:

1. Безопасность. Образование. Человек: информационный портал ОБЖ и БЖД: Информационный портал http://window.edu.ru/resource/009/67009
2. Журнал «Основы безопасности жизнедеятельности»: Электронный ресурс http://www.school-obz.org
3. Портал МЧС России: Электронный ресурс http://www.mchs.gov.ru.
4. Энциклопедия безопасности: Информационный ресурс http://www.opasno.net/

Современные профессиональные базы данных и информационно-справочные системы:

1. ЭБС «Университетская библиотека онлайн».
2. Коллекция Шуйского филиала ИвГУ на национальном цифровом ресурсе «Руконт».

Программное обеспечение:

В процессе изучения дисциплины «Информационная безопасность» используются офисные пакеты Microsoft Office, Open Office, программа для просмотра и чтения файлов PDF Adobe Acrobat Reader DC, программа для воспроизведения флэш-анимации в браузерах Adobe Flash Player, вэб-обозреватели Google Chrome, Opera, Антивирус Касперского, 1С университет.

9. Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного типа, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории.

2. Учебная аудитория для проведения занятий семинарского типа, укомплектованная специализированной мебелью и техническими средствами обучения.

3. Учебная аудитория для проведения групповых и индивидуальных консультаций, укомплектованная специализированной мебелью и техническими средствами обучения.

4. Учебная аудитория для проведения текущего контроля и промежуточной аттестации, укомплектованная специализированной мебелью и техническими средствами обучения.

5. Помещение для самостоятельной работы, оснащенное специализированной мебелью, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

6. Учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации: электронные презентации, видеоматериалы, модели органов человека.

Автор(ы) рабочей программы дисциплины:

В.И. Гинко, доцент кафедры безопасности жизнедеятельности и адаптивной физической культуры, кандидат педагогических наук, доцент.

Программа рассмотрена на заседании кафедры безопасности жизнедеятельности и адаптивной физической культуры

«25» апреля 2019 г., протокол № 8

Программа обновлена
протокол заседания кафедры № 8 от «27» февраля 2020 г.
Согласовано:



Программа обновлена
протокол заседания кафедры № 11 от «11» июня 2021 г.
Согласовано:



Программа обновлена
протокол заседания кафедры № 6 от «21» января 2022 г.
Согласовано:



Программа обновлена
протокол заседания кафедры № 10 от «29» июня 2023 г.
Согласовано:



Приложение 1

Методические указания для обучающихся по освоению дисциплины

Задания для практической работы

Тема 1. «История и современные направления развития информационной безопасности»
Вопросы и задания:

1. История развития средств и методов защиты информации.
2. Основные этапы решения проблем защиты информации.
3. Защита от информационного воздействия.
4. Информационная война.
5. Понятие информационной безопасности.

Литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
2. Петров, С.В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.

Тема 2. «Система организационно-правового обеспечения информационной безопасности»
Вопросы и задания:

1. Система защиты информации.
2. Структура государственной системы защиты информации.
3. Основные субъекты государственной системы защиты информации.
4. Государственная система организационно-правового обеспечения информационной безопасности.

Литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
2. Петров, С.В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.

Тема 3. «Правовая основа информационной безопасности»
Вопросы и задания:

1. Требования к законодательству в области информационной безопасности

2. Правовая основа обеспечения информационной безопасности в России.
3. Конституция и законодательные акты РФ о защите информации.
4. Регламентирование вопросов защиты информации в ведомственных нормативных актах.
5. Ответственность за нарушение требований защиты информации.

Литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
2. Петров, С.В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.

Тема 4. «Источники угроз защищаемой информации»

Вопросы и задания:

1. Классификация и содержание возможных угроз информации.
2. Причины и условия утечки защищаемой информации.
3. Способы незаконного получения защищаемой информации.

Литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
2. Петров, С.В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.

Тема 5. «Криминалистическая характеристика способов незаконного получения защищаемой информации»

Вопросы и задания:

1. Похищение документов, содержащих защищаемые сведения.
2. Незаконное получение конфиденциальной информации.

Литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-

4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
2. Петров, С.В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.

Тема 6. «Принципы защиты информации»

Вопросы и задания:
1. Правовые принципы защиты информации.
2. Организационные принципы защиты информации.
3. Специфические принципы защиты информации.

Литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
2. Петров, С.В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.

Тема 7. «Мероприятия, методы и средства защиты информации»

Вопросы и задания:
1. Понятие защиты информации.
2. Мероприятия по защите информации.
3. Методы защиты информации.
4. Способы защиты информации.
5. Средства защиты информации.

Литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
2. Петров, С.В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.

Тема 8. «Понятие защищаемой информации»

Вопросы и задания:
1. Особенности защищаемой информации.

2. Носители защищаемой информации.
3. Классификация защищаемой информации.

Литература

1. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=363040
2. Петров, С.В. Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, П. А. Кисляков ; Министерство образования и науки РФ; ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы. - Москва : Русский журнал, 2011. - 328 с.

Темы рефератов

1. Понятие, свойства и структура информации.
2. Объекты и субъекты информационной безопасности.
3. Концептуальная модель информационной безопасности.
4. Угрозы конфиденциальной информации.
5. Правовая защита информационной безопасности.
6. Защита информации утечки по техническим каналам.
7. Противодействие несанкционированному доступу к источникам информации.
8. Взаимодействие с зарубежными партнерами и информационная безопасность.
9. Аудит информационной безопасности.
10. Информационные угрозы террористического характера.
11. История информационных войн.
12. Информационные войны и государственная власть.
13. Кибертерроризм – угроза информационной безопасности.
14. Обеспечение информационной безопасности несовершеннолетних.
15. Проблемы региональной информационной безопасности.
16. Политика безопасности глобальной сети Интернет.
17. Безопасность в социальных сетях.
18. Информационные аспекты безопасности семейных отношений.
19. Информационные противостояния в сфере межличностного взаимодействия.
20. Роль и возможности России в глобальном информационном обществе.
21. Информационные угрозы и здоровье молодежи. Современные виды нехимической зависимости.
22. Слухи как фактор возникновения паники в обществе.
23. Политические и рекламные кампании и их влияние на информационную безопасность общества.
24. Обеспечение информационной безопасности личности.
25. Обеспечение информационной безопасности общества.
26. Обеспечение информационной безопасности государства.
27. Права и обязанности граждан в информационной сфере.
28. Ответственность за правонарушения в информационной сфере.

Требования к реферату

Объем – 10-15 страниц (шрифт Times New Roman, формат А4 (210х297 мм), кегль 14, межстрочный интервал одинарный, поля слева 25 мм, с других сторон – по 20 мм, без переносов, абзацный отступ 1,25, выравнивание текста по ширине).
Во введении должны присутствовать актуальность темы, цель и задачи. В заключении необходимо отразить выводы по задачам. Список использованной литературы должен включать не менее пяти источников (ссылки на эти источники обязательны).
Структура реферата:

1. Титульный лист
2. Содержание
3. Введение
4. Основная часть

4.1…..
4.2…..

5. Заключение
6. Список использованной литературы