МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института энергетики, информационных технологий и управляющих систем
_____ Белоусов А.В.
«20» мая 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Расследование инцидентов информационной безопасности

направление подготовки:

10.05.03 Информационная безопасность автоматизированных систем

Специализация программы:

Безопасность открытых информационных систем

Квалификация

Специалист по защите информации

Форма обучения

очная

Институт энергетики, информационных технологий и управляющих систем

Кафедра Программного обеспечения вычислительной техники и автоматизированных систем

Белгород 2021

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Минобрнауки России от 26.11.2020 №1457
- учебного плана, утвержденного ученым советом БГТУ им. В.Г. Шухова в 2021 году.

Составитель: к.т.н., доцент _____ (Гаврющенко А.П.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

« 14 » 05 2021 г., протокол № 8

Заведующий кафедрой: к.т.н., доцент _____ (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой программного обеспечения вычислительной техники и автоматизированных систем
(наименование кафедры/кафедр)

Заведующий кафедрой: к.т.н., доцент _____ (Поляков В.М.)
(ученая степень и звание, подпись) (инициалы, фамилия)

« 14 » 05 2021 г.

Рабочая программа одобрена методической комиссией института

« 20 » 05 2021 г., протокол № 9

Председатель к.т.н., доцент _____ (Семернин А.Н.)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания результата обучения по дисциплине
Профессиональные компетенции	ПК-3 Способен выполнять анализ и постановку новых задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации (научно-исследовательский)	ПК-3.1 Выполняет анализ компьютерных инцидентов в целях постановки задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации	**Знать:** основные методы исследования компьютерных систем на предмет вскрытия инцидента информационной безопасности; **Уметь:** вырабатывать правильные решения по реагированию на инциденты информационной безопасности; **Владеть:** навыками постановки задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1. Компетенция ПК-3 Способен выполнять анализ и постановку новых задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации.

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименования дисциплины
1.	Основы искусственного интеллекта
2.	Промышленный интернет
3.	Интеллектуальный анализ больших данных
4.	Технология построения защищенных распределенных приложений
5.	Практикум по подготовке инженерной документации
6.	Анализ рисков информационной безопасности

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зач. единиц, 144 часов.

Форма промежуточной аттестации: зачет.

Вид учебной работы	Всего часов	Семестр № 6
Общая трудоемкость дисциплины, час	144	144
Контактная работа (аудиторные занятия), в т.ч.:	71	71
лекции	34	34
лабораторные	17	17
практические	17	17
групповые консультации в период теоретического обучения и промежуточной аттестации	3	3
контроль самостоятельной работы	-	-
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	73	73
Курсовой проект	-	-
Курсовая работа	-	-
Расчетно-графическое задания	-	-
Индивидуальное домашнее задание	-	-
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	73	73
Зачет	-	-

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4.1 Наименование тем, их содержание и объем
Курс 5 Семестр 9

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1.	Правовая база расследования компьютерных правонарушений и инцидентов информационной безопасности.				
	Цель и задачи курса. Содержание дисциплины. Рекомендуемая литература. Порядок изучения дисциплины. Понятия компьютерного преступления и инцидента информационной безопасности. Классификация правонарушений в компьютерной сфере. Криминалистическая характеристика правонарушений в компьютерной сфере.	8	4	-	18
2.	Основные мероприятия расследования компьютерных правонарушений и инцидентов информационной безопасности.				
	Возбуждение уголовных дел по преступлениям в сфере высоких технологий. Привлечение к расследованию специалистов. Осмотр места происшествия, выемка и осмотр средств компьютерной техники и носителей информации. Осмотр электронных документов. Оперативно-розыскные мероприятия. Назначение компьютерной экспертизы.	8	4	4	18
3.	Организация реагирования на инциденты информационной безопасности.				
	Стандарты и общий цикл управления инцидентами ИБ. Средства обнаружения инцидентов ИБ. Правовые основания использование данных мониторинга и DLP-систем. Первичное реагирование на инцидент ИБ. Процедура сбора свидетельств инцидента ИБ. Группа реагирования на инциденты.	10	5	9	19
4.	Методы и средства исследования компьютерных систем.				
	Криминалистические исследования компьютерных систем. Инструменты снятия данных. Инструменты криминалистического анализа компьютерных систем.	8	4	4	18
	ВСЕГО	34	17	17	73

4.2. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема практического занятия	К-во часов	К-во часов СРС
семестр № 9				
1.	Правовая база расследования компьютерных правонарушений и	Понятия компьютерного преступления и инцидента информационной безопасности.	2	2
		Классификация правонарушений в	2	2

	инцидентов информационной безопасности.	компьютерной сфере. Криминалистическая характеристика правонарушений в компьютерной сфере.		
2.	Основные мероприятия расследования компьютерных правонарушений и инцидентов информационной безопасности	Возбуждение уголовных дел по преступлениям в сфере высоких технологий. Привлечение к расследованию специалистов.	2	2
		Оперативно-розыскные мероприятия. Назначение компьютерной экспертизы.	2	2
3.	Организация реагирования на инциденты информационной безопасности	Стандарты и общий цикл управления инцидентами ИБ. Группа реагирования на инциденты.	3	3
		Средства обнаружения инцидентов ИБ. Правовые основания использование данных мониторинга и DLP-систем.	2	2
4.	Методы и средства исследования компьютерных систем.	Выявление элементов инфраструктуры, затронутых инцидентом. Криминалистические исследования компьютерных систем.	2	2
		Инструменты снятия данных. Инструменты криминалистического анализа компьютерных систем.	2	2
ИТОГО:			17	17
ВСЕГО:				34

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема практического занятия	К-во часов	К-во часов СРС
семестр № 9				
1.	Основные мероприятия расследования компьютерных правонарушений и инцидентов информационной безопасности	Осмотр места происшествия, выемка и осмотр средств компьютерной техники и носителей информации. Осмотр электронных документов.	4	4
2.	Организация реагирования на инциденты информационной безопасности	Первичное реагирование на инцидент ИБ.	4	4
		Процедура сбора свидетельств инцидента ИБ.	5	5
3.	Методы и средства исследования компьютерных систем.	Выявление элементов инфраструктуры, затронутых инцидентом.	4	4
ИТОГО:			17	17
ВСЕГО:				34

4.4. Содержание курсового проекта/работы

Не предусмотрено учебным планом

4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Не предусмотрено учебным планом

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенций

1. Компетенция ПК-3 Способен выполнять анализ и постановку новых задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации

Наименование индикатора достижения компетенции	Используемые средства оценивания
ПК-3.1 Выполняет анализ компьютерных инцидентов в целях постановки задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации	собеседование на практическом и лабораторном занятии, зачет

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Правовая база расследования компьютерных правонарушений и инцидентов информационной безопасности	Понятие преступления в сфере компьютерной информации. Основные федеральные законы в сфере информационной безопасности. Классификация информации ограниченного доступа. Понятие несанкционированного доступа к информации. Понятие правил разграничения доступа. Понятие вредоносного программного обеспечения. Понятие компьютерного инцидента по отношению к КИИ. СВТ, ЭВМ, вычислительная машина, компьютерная информация. Классификация правонарушений в компьютерной сфере. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем. Преступления, связанные с контентом. Преступления, связанные с правами собственности и товарными знаками. Преступления, связанные с применением компьютерной техники. Комбинированные преступления.
2.	Основные мероприятия расследования компьютерных правонарушений и инцидентов информационной безопасности	Каким может быть повод для возбуждения уголовных дел по преступлениям в сфере высоких технологий? Алгоритм расследования компьютерных преступлений. Привлечение к расследованию специалистов. Осмотр места происшествия, выемка и осмотр средств компьютерной техники и носителей информации. Осмотр электронных документов. Оперативно-розыскные мероприятия: перехват и исследование сетевого трафика, использование кейлогеров, поиск информации в открытых источниках, определение принадлежности IP адресов, определение принадлежности доменных имен, определение принадлежности адреса электронной почты. Назначение компьютерной экспертизы.
3.	Организация реагирования на инциденты информационной безопасности	ГОСТы в области управления инцидентами информационной безопасности. Понятие события, инцидента информационной безопасности. Этапы управления инцидентами ИБ. Средства обнаружения инцидентов ИБ. Мероприятия, способствующие эффективной обработке инцидентов ИБ. Правовые основания использование данных мониторинга и DLP-систем. Первичное реагирование на инцидент ИБ. Типовой сценарий при нарушениях ИБ.

		Процедура сбора свидетельств инцидента ИБ. Группа реагирования на инциденты.
4.	Методы и средства исследования компьютерных систем.	Выявление элементов инфраструктуры, затронутых инцидентом. Криминалистические исследования компьютерных систем. Понятие форензики. Инструменты снятия данных. Создание образа носителя информации. Снятие энергозависимых данных. Инструменты криминалистического анализа компьютерных систем.

5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

Текущий контроль осуществляется в течение семестра в форме собеседования и устного опроса.

Собеседования и устные опросы направлены на проверку степени усвоения материала и понимания теоретических сведений, используемых в процессе выполнения работы. Примерные перечень вопросов для контроля знаний приведен в таблице:

Тематика дисциплины	Контрольные вопросы
Правовая база расследования компьютерных правонарушений и инцидентов информационной безопасности	1. Дать понятие преступления в сфере компьютерной информации. 2. Перечислить основные федеральные законы в сфере информационной безопасности. 3. Дать классификацию информации ограниченного доступа. 4. Понятие несанкционированного доступа к информации. 5. Понятие правил разграничения доступа. 6. Понятие вредоносного программного обеспечения. 7. Понятие компьютерного инцидента по отношению к КИИ. 8. СВТ, ЭВМ, вычислительная машина, компьютерная информация. 9. Классификация правонарушений в компьютерной сфере. 10. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем. 11. Преступления, связанные с контентом. 12. Преступления, связанные с правами собственности и товарными знаками. 13. Преступления, связанные с применением компьютерной техники. 14. Комбинированные преступления.
Основные мероприятия расследования компьютерных правонарушений и инцидентов информационной безопасности	1. Каким может быть повод для возбуждения уголовных дел по преступлениям в сфере высоких технологий? 2. Алгоритм расследования компьютерных преступлений. 3. Привлечение к расследованию специалистов. 4. Осмотр места происшествия. 5. Выемка и осмотр средств компьютерной техники и носителей информации. 6. Осмотр электронных документов. 7. Оперативно-розыскные мероприятия: перехват и исследование сетевого трафика. 8. Оперативно-розыскные мероприятия: использование кейлогеров. 9. Оперативно-розыскные мероприятия: поиск информации в открытых источниках. 10. Оперативно-розыскные мероприятия: определение принадлежности IP адресов. 11. Оперативно-розыскные мероприятия: определение принадлежности доменных имен.

	12. Оперативно-розыскные мероприятия: определение принадлежности адреса электронной почты. 13. Назначение компьютерной экспертизы.
Организация реагирования на инциденты информационной безопасности	1. ГОСТы в области управления инцидентами информационной безопасности. 2. Понятие события информационной безопасности. 3. Понятие инцидента информационной безопасности. 4. Этапы управления инцидентами ИБ. 5. Средства обнаружения инцидентов ИБ. 6. Межсетевые экраны. 7. Системы обнаружения / предотвращения вторжений 8. антивирусные средства. 9. системы защиты от утечек информации. 10.Журналы сетевых устройств. 11.Мероприятия, способствующие эффективной обработке инцидентов ИБ. 12.Правовые основания использование данных мониторинга и DLP-систем. 13.Первичное реагирование на инцидент ИБ. 14.Типовой сценарий при нарушениях ИБ. 15.Процедура сбора свидетельств инцидента ИБ. 16.Группа реагирования на инциденты.
Методы и средства исследования компьютерных систем.	1. Выявление элементов инфраструктуры, затронутых инцидентом. 2. Что такое индикатор компрометации. 3. Криминалистические исследования компьютерных систем. 4. Действия аналитиков в ходе расследования. 5. Понятие форензики. 6. Структура процесса криминалистического исследования компьютерных систем. 7. Инструменты снятия данных. 8. Создание образа носителя информации. 9. Снятие энергозависимых данных. 10. Инструменты криминалистического анализа компьютерных систем.

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме зачета используется следующая шкала оценивания: 2 – неудовлетворительно, 3 – удовлетворительно, 4 – хорошо, 5 – отлично.

Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Знание терминов, определений, понятий
	Знание основных закономерностей, соотношений, принципов
	Объем освоенного материала
	Полнота ответов на вопросы
	Четкость изложения и интерпретации знаний

Умения	Умение анализировать основные положения законодательства в области безопасности информации
	Умение использовать руководящие документы регуляторов в области информационной безопасности
Навыки	Владение навыками теоретического и экспериментального исследования объектов профессиональной деятельности
	Качество выполнения исследований объектов профессиональной деятельности
	Самостоятельность выполнения исследований объектов профессиональной деятельности

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Знание терминов, определений, понятий	Не знает терминов и определений	Знает термины и определения, но допускает неточности формулировок	Знает термины и определения	Знает термины и определения, может корректно сформулировать их самостоятельно
Знание основных закономерностей, соотношений, принципов	Не знает основные закономерности и соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний, их интерпретирует и использует	Знает основные закономерности, соотношения, принципы построения знаний, может самостоятельно их получить и использовать
Объем освоенного материала	Не знает значительной части материала дисциплины	Знает только основной материал дисциплины, не усвоил его деталей	Знает материал дисциплины в достаточном объеме	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает неполные ответы на все вопросы	Дает ответы на вопросы, но не все - полные	Дает полные, развернутые ответы на поставленные вопросы
Четкость изложения и интерпретации знаний	Излагает знания без логической последовательности	Излагает знания с нарушениями в логической последовательности	Излагает знания без нарушений в логической последовательности	Излагает знания в логической последовательности, самостоятельно их интерпретируя и анализируя
	Не иллюстрирует изложение поясняющими схемами, рисунками и примерами	Выполняет поясняющие схемы и рисунки небрежно и с ошибками	Выполняет поясняющие рисунки и схемы корректно и понятно	Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний
	Неверно излагает и интерпретирует знания	Допускает неточности в изложении и	Грамотно и по существу излагает знания	Грамотно и точно излагает знания, делает

		интерпретации знаний		самостоятельные выводы

Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Умение осуществлять формирование требований к защите информации автоматизированных систем	Не умеет осуществлять формирование требований к защите информации автоматизированных систем	Допускает неточности в осуществлении формирования требований к защите информации автоматизированных систем	Умеет осуществлять формирование требований к защите информации автоматизированных систем	Умеет осуществлять формирование требований к защите информации автоматизированных систем и делать обобщающие выводы
Умение выполнять анализ компьютерных инцидентов в целях постановки задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации	Не умеет выполнять анализ компьютерных инцидентов в целях постановки задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации	Выполнение анализа компьютерных инцидентов в целях постановки задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации вызывает затруднения	Умеет выполнять анализ компьютерных инцидентов в целях постановки задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации	Умело выполняет анализ компьютерных инцидентов в целях постановки задач в области разработки математического, алгоритмического и программного обеспечения систем защиты информации

Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка			
	2	3	4	5
Владение навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Не владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Не достаточно хорошо владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности	Профессионально владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности
Качество выполнения исследований объектов профессиональной деятельности	Не качественно выполняет исследования объектов профессиональной деятельности, допускает грубые ошибки	Не достаточно качественно выполняет исследования объектов профессиональной деятельности, допускает и	Не достаточно качественно выполняет исследования объектов профессиональной деятельности, допускает и	Качественно выполняет исследования объектов профессиональной деятельности

		исправляет ошибки с посторонней помощью	исправляет ошибки самостоятельно	
Самостоятельность выполнения исследований объектов профессиональной деятельности	Не может самостоятельно выполнять исследования объектов профессиональной деятельности	Выполняет исследования объектов профессиональной деятельности с посторонней помощью	При выполнении исследования объектов профессиональной деятельности иногда требуется посторонняя помощь	Самостоятельно выполняет исследования объектов профессиональной деятельности

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Материально-техническое обеспечение

№	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1.	Учебная аудитория для проведения лекционных занятий	Специализированная мебель. Мультимедийная установка, экран, доски
2.	Учебная аудитория для проведения практических занятий	Специализированная мебель. Компьютеры на базе процессоров Intel или AMD.
3.	Читальный зал библиотеки для самостоятельной работы	Специализированная мебель. Компьютерная техника, подключенная к сети интернет и имеющая доступ в электронно-образовательную среду.

6.2. Лицензионное и свободно распространяемое программное обеспечение

№	Перечень лицензионного программного обеспечения.	Реквизиты подтверждающего документа
1	Microsoft Windows 10 Корпоративная	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
2	Microsoft Office Professional Plus 2016	(Соглашение Microsoft Open Value Subscription V9221014 Соглашение действительно с 01.11.2020 по 31.10.2023). Договор поставки ПО № 128-21 от 30.10.2021.
3	Kaspersky Endpoint Security «Стандартный Russian Edition»	Сублицензионный договор № 102 от 24.05.2018. Срок действия лицензии до 19.08.2020 Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования (лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2022г.
4	Среды программирования Free Pascal, Dev C++ или CodeBlocks	Свободно распространяемое ПО согласно условиям лицензионного соглашения

6.3. Перечень учебных изданий и учебно-методических материалов

1. Башлы П.Н. Информационная безопасность: учебно-практическое пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К. - М.: Изд. центр ЕАОИ, 2011. - 376 с. http://www.biblioclub.ru/book/90539/

2. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.html.— ЭБС «IPRbooks»

3. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности. [Электронный ресурс] : Учебные пособия / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков. — Электрон. дан. — СПб. : НИУ ИТМО, 2013. — 148 с. — Режим доступа: http://e.lanbook.com/book/43579

4. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности. [Электронный ресурс] : Учебные пособия — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 140 с. — Режим доступа: http://e.lanbook.com/book/5163

5. Креопалов В. В. Технические средства и методы защиты информации: учебно-практическое пособие / В.В. Креопалов. - М.: Изд. центр ЕАОИ, 2011.- 278 с. http://www.biblioclub.ru/book/90753/

6. Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации и информационной сфере / Н.Н. Куняев. — М.: Логос, 2010. - 348 с. http://www.biblioclub.ru/book/84990/

7. Ярочкин В.И. Информационная безопасность [Электронный ресурс]: учебник для вузов/ Ярочкин В.И.— Электрон. текстовые данные.— М.: Академический Проект, 2008.— 544 с.— Режим доступа: http://www.iprbookshop.ru/36331.html.— ЭБС «IPRbooks»

8. Алешенков М. Основы национальной безопасности/М.Алешенков /Основы безопасности жизни.-2005.-№11.-С.5-10. [текст]

9. Брандман Э. М. Глобализация и информационная безопасность общества/Э.М.Брандман //Философия и общество.-2006.-№1.-С.31-41. [текст]

10. Брандман Э. М. Цивилизационные императивы и приоритеты информационной безопасности общества/Э.М.Брандман //Философия и общество.-2006.-№3.-С.60-77..-Предпринимательство, с.131-144. [текст]

11. Доктрина информационной безопасности //Средства массовой информации постсоветской России: Учеб. пособие /Я.Н. Засурский, Е. Л. Вартанова, И.И. Засурский.-М., 2002.-С.262-301. [текст]

12. Егозина В. Смотреть нельзя запретить (агрессивная информационная среда как угроза для безопасности)/В. Егозина, Н. Овчинников //ОБЖ.- 2003.-№4.-С.15-18. [текст]

13. Еляков А.Д. Информационная свобода человека/А.Д.Еляков // Социально-гуманитарные знания.-2005.-№3.-С.125-141. [текст]

14. Жигулин, Г.П. Организационное и правовое обеспечение информационной безопасности. [Электронный ресурс] : Учебные пособия — Электрон. дан. — СПб. : НИУ ИТМО, 2014. — 173 с. — Режим доступа:

http://e.lanbook.com/book/70952

15. Кожуханов, Н.М. Правовые основы информационной безопасности: учебное пособие. [Электронный ресурс] : Учебные пособия / Н.М. Кожуханов, Е.С. Недосекова. — Электрон. дан. — М. : РТА, 2013. — 88 с. — Режим доступа: http://e.lanbook.com/book/74237

16. Мамаев С.М., Петренко.Технологии защиты информации в Интернете. Санкт-Петрбург, Изд-во «ПИТЕР». Москва-Харьков-Минск. 2002г.[текст]

17. Морозов И. Л. Информационная безопасность политической системы / И.Л.Морозов //ПОЛИС.-2002.-№5.-С.134-146. [текст]

18. Норткат С., Новак Д.- Обнаружение нарушений безопасности в сетях. Изд-й дом Вильямс, 2003г. [текст]

19. Поляков В. П. Практическое занятие по изучению вопросов информационной безопасности/В.П.Поляков //Информатика и образование.-2006.-№11.-С.75-80. [текст]

20. Поляков В.П. Информационная безопасность в курсе информатики /В.П.Поляков //Информатика и образование.-2006.-№10.-С.116-119.[текст]

Нормативные документы

1. Всеобщая декларация прав человека (от 10 декабря 1948 г.). М., 2010.
2. Конституция РФ. М., 2010.
3. Гражданский кодекс РФ. М., 2010.
4. Доктрина информационной безопасности РФ. М., 2010.
5. Федеральный закон «О государственной тайне» от 21 июля 1993 г. № 5485-1. М., 1993.
6. Федеральный закон «Об авторском праве и смежных правах» от 9 июля 1993 г. № 5351-1 (с последующими изменениями). М., 1993.
7. Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 г. № 1-ФЗ. М., 2002.
8. Закон Российской Федерации от 21.07.1993г. № 5485-1 «О государственной тайне». // Российская газета от 21.09.1992г.
9. Федеральный закон РФ от 10.01.2002г. № 1-ФЗ «Об электронной цифровой подписи» // Российская газета, 12.01.2002.
10. ГОСТ РВ 51987-02 «Типовые требования и показатели качества функционирования информационных систем».
11. ГОСТ Р ИСО/МЭК 15408-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

12. ГОСТ Р ИСО/МЭК 27001-2006. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента в информационной безопасности. Требования». М.: ИПК Издательство стандартов, 2007.

6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем

1. Электронная библиотека (на базе ЭБС «БиблиоТех») — Режим доступа:

http://ntb.bstu.ru

2. Электронно-библиотечная система IPRbooks — Режим доступа: http://www.iprbookshop.ru
3. Электронно-библиотечная система «Университетская библиотека ONLINE» — Режим доступа: http://www.biblioclub.ru/
4. http:// www.consultantplus.ru/ - нормативно-правовая база
5. http://www.garant.ru/ - нормативно-правовая база
6. http://www.promo.s-director.ru/ – сайт журнала «Директор по безопасности»
7. http://college.ru/UDP/texts/ – учебный курс «Защита информации»;
8. http://www.mirash.ru/doki11.html - нормативная база по защите информации;
9. http://tk.plexor.ru/web-links/info/38-zakon.html - нормативные документы по защите информации.
10. http://www.inattack.ru/ - антивирусное программное обеспечение
11. http://securityvulns.ru/ - нормативные документы по защите информации
12. http://www.glossary.ru/cgi-bin/gl_sch2.cgi?RIt(uwsg.outtg9!hlnuvgxtuxy
13. http://www.gosecure.ru/ - сайт форматов ЭЦП
14. http://z-oleg.com/ - антивирусное программное обеспечение
15. http://www.aladdin.ru/ - сайт производителя средств защиты информации

7. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа утверждена на 202__/202__ учебный год без изменений / с изменениями, дополнениями

Протокол № _____ заседания кафедры от «____»_____ 202_ г.

Заведующий кафедрой_____
подпись, ФИО

Директор института _____
подпись, ФИО