МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра уголовного права

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«____» _____ 2019 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для самостоятельной работы по изучению дисциплины
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для студентов специальности
40.05.02 Правоохранительная деятельность

Курск 2019

УДК 65.01 : 330.131

Составители: И.А. Шуклин, Р.Ф. Шахбазов

Рецензент
Доктор юридических наук, профессор _____

Методические указания для самостоятельной работы по изучению дисциплины «Основы информационной безопасности» для студентов специальности 40.05.02 Правоохранительная деятельность / сост. Шуклин И.А., Шахбазов Р.Ф.: Юго-Зап. гос. ун-т. Курск, 2019. 121 с.

Методические указания составлены на основании учебного плана специальности 40.05.02 Правоохранительная деятельность и рабочей программы дисциплины «Основы информационной безопасности».

Включают общие положения, широкий набор различных видов работы обучающихся при освоении дисциплины: содержание лекционных, практических занятий и самостоятельной работы студентов, формы контроля и требования к оценке знаний по дисциплине, список рекомендуемой литературы и информационное обеспечение дисциплины. Обеспечивают необходимые задания и критерии оценки, как для аудиторной, так и самостоятельной работы студентов, которая играет особую роль в подготовке специалистов.

Методические указания помогают сформировать студентам знания и навыки в области использования компьютерных информационных технологий в сфере информационной безопасности и профессиональными компетенциями в объеме осваиваемых видов и задач профессиональной деятельности, предусмотренных требованиями ФГОС ВО в результате изучения дисциплины.

Предназначены для студентов всех форм обучения по специальности 40.05.02 Правоохранительная деятельность и будут полезны преподавателям при организации образовательной деятельности.

Текст печатается в авторской редакции

Подписано в печать . Формат 60х84 1/16.
Усл. печ. л. . Уч.-изд. л. . Тираж 100 экз. Заказ Бесплатно.
Юго-Западный государственный университет
305040, г. Курск, ул. 50 лет Октября, 94.

ОГЛАВЛЕНИЕ

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ ПОЛОЖЕНИЯ

1.1. Общие положения

Учебная дисциплина Б1.В.ДВ.04.01 «Основы информационной безопасности» определена в качестве дисциплины по выбору базовой части учебного плана ООП по специальности 40.05.02 Правоохранительная деятельность, утвержденного Ученым советом университета 26 марта 2018 года (протокол №9).

Дисциплина представляет собой дидактически обоснованную систему знаний, обеспечивающую формирование умений и навыков для освоения соответствующих общекультурных и профессиональных компетенций, предусмотренных требованиями ФГОС ВО по данной специальности.

Цель дисциплины – формирование у обучающихся целостной системы базовых теоретических знаний основ информационной безопасности и практических умений использования современных методов обработки, преобразования и защиты информации в современных компьютерных системах, а также овладения студентами соответствующими общекультурными и профессиональными компетенциями в объеме осваиваемых видов и задач профессиональной деятельности, предусмотренных требованиями ФГОС ВО.

Предмет дисциплины:

- информационная безопасность как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;
- обеспечение информационной безопасности как осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию,

обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

- система обеспечения информационной безопасности как совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

Основные задачи дисциплины:

- приобретение обучающимися необходимых познаний в сфере информационной безопасности в контексте решения профессиональных задач по профилю юридической деятельности;
- формирование у обучающихся способностей соблюдения в профессиональной деятельности требований нормативных правовых актов в области информационной безопасности;
- получение обучающимися навыков в применении основных методов, способов и средств получения, хранения, поиска, систематизации, обработки, передачи и защиты информации при решении профессиональных задач в объеме предусмотренных ФГОС ВО видов профессиональной деятельности;
- развитие способностей обучающихся в работе с различными информационными ресурсами и применении современных способов борьбы с несанкционированным блокированием, доступом, копированием, изменением и сбором информации.

Дисциплина формирует профессиональную компетентность ПК-22 – способность выпускника соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности.

В результате изучения данного курса студенты должны:

знать:

- - основные закономерности создания и функционирования информационных процессов в правовой сфере;
- основы государственной политики в области информатики;
- методы и средства поиска, систематизации и обработки правовой информации;
- практические способы построения систем защиты информации;

- нормативные правовые акты в области защиты информации и противодействия техническим разведкам;

- основные положения Стратегии национальной безопасности Российской Федерации;

- основные положения Доктрины информационной безопасности Российской Федерации в части угроз и опасностей, стратегии и тактики, внешних и внутренних факторов, влияющих на состояние национальной безопасности;

- информационные угрозы, их виды;

- формальные и неформальные методы и средства защиты информации;

- технические и программные методы и средства защиты информации;

- понятие конфиденциальности и целостности информации, причины их нарушения;

- основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности;

-ограничение доступа к информации: идентификация, авторизация, аутентификация, криптографические преобразования;

- вредоносные программы и их виды;

- средства борьбы с вредоносными программами

- основные методы, способы и мероприятия по обеспечению информационной безопасности в профессиональной деятельности;

уметь:

- применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов и проведения статистического анализа правовой и служебной информации;

- оперировать информационными понятиями и категориями;

- строить системы защиты информации;

- осуществлять формирование режима информационной безопасности;

- определять необходимую степень защиты информации;

- принимать меры по защите информации, содержащейся в технических устройствах, от негативного воздействия

- использовать методы и средства обеспечения информационной безопасности с целью предотвращения

несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации;

владеть навыками:

- сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности;
- обеспечения режима информационной безопасности в организации;
- организации достоверной, безопасной передачи информации в компьютерных и других информационных систем связи.
- обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, злоумышленной модификации или утраты информации, составляющей государственную тайну и иной служебной информации.

1.2. Объем дисциплины и виды учебной работы

Объём дисциплины и виды учебной работы определены учебным планом специальности 40.05.02 Правоохранительная деятельность. Общая трудоемкость (объем) дисциплины составляет 3 зачетных единиц (з.е.), 108 часов. Распределение часов по темам лекционных, практических занятий и самостоятельной работы студентов представлено в таблице 1.

Таблица 1 – Содержание дисциплины и её трудоёмкость в часах и зачётных единицах (ЗЕ) (для очной формы обучения)

№ п/п	Наименование темы	Вид проводимого занятия		Самостоятельная работа студента (объем в часах)
		лекция	практика	
1	Введение в дисциплину «Основы информационной безопасности»	2	4	6
2	Сущность проблемы информационной безопасности (ИБ)	2	4	6
3	Основные угрозы информационной безопасности	2	4	6
4	Правовое обеспечение информационной	2	4	6

	безопасности			
5	Организационное обеспечение информационной безопасности	2	4	6
6	Защита информации в компьютерных системах от случайных угроз и традиционного шпионажа	2	4	6
7	Методы и средства защиты информации от несанкционированного доступа и изменения структур в компьютерных системах	2	4	6
8	Защита информации в распределенных компьютерных системах	2	4	6
9	Защита компьютерных систем от вирусов и вредоносных программ	2	4	6
	Общая трудоемкость (час) / ЗЕ	54 ч / 1,5 ЗЕ		54 ч / 1,5 ЗЕ
	Форма контроля	зачёт		
	ВСЕГО по дисциплине	108 часов / 3 ЗЕ		

1.3. Методические рекомендации по организации изучения дисциплины

В рамках изучения дисциплины «Основы информационной безопасности» работа студентов организуется в следующих формах:

1) работа с конспектом лекций и дополнительной литературой по темам курса;

2) работа с раздаточным материалом – «Скрин-шот»;

3) изучение вопросов, выносимых за рамки лекционных занятий (дискуссионные вопросы для дополнительного изучения);

4) подготовка к практическому занятию;

5) выполнение групповых и индивидуальных домашних заданий, в том числе: проведение собеседования по теме лекции; подготовка краткого доклада (резюме, эссе) по заданной теме и разработка мультимедийной презентации к нему; выполнение практических заданий (решение задач, выполнение расчетных работ); подготовка к тестированию;

6) самоконтороль.

Рекомендуемый ниже режим самостоятельной работы позволит студентам глубоко разобраться во всех изучаемых вопросах, активно

участвовать на практических занятиях и в конечном итоге успешно сдать зачёт по дисциплине «Правовая информатика».

1. *Лекция* является фундаментальным источником знаний для реализации этапа формирования знаниевой компоненты осваиваемых компетенций и должна способствовать глубокому усвоению материала, активизировать интерес студента к изучаемой дисциплине.

Работу с конспектом лекций целесообразно проводить непосредственно после её прослушивания. Она предполагает перечитывание конспекта, внесение в него, по необходимости, уточнений, дополнений, разъяснений и изменений. Ознакомление с дополнительной литературой по теме, проведение обзора мнений других ученных по изучаемой теме. Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологии (понятий), категорий и законов (глоссарий к каждой теме содержится в разделе 2 настоящих методических указаний). Студенту рекомендуется не ограничиваться при изучении темы только конспектом лекций или одним учебником; необходимо не только конспектировать лекции, но и читать дополнительную литературу, изучать методические рекомендации, издаваемые кафедрой.

2. *«Скрин-шот»* – специальный раздаточный материал, подготовленный преподавателем, который предназначен для повышения эффективности учебного процесса за счет:

1) привлечения дополнительного внимания студента на наиболее важных и сложных проблемах курса;

2) освобождения от необходимости ведения рутинных записей по ходу лекции и возможности более адекватной фиксации ключевых положений лекции;

3) представления всего необходимого иллюстративного и справочно-информационного материала по теме лекции;

4) более глубокой переработки материалов курса при подготовке к зачету или экзамену.

Самостоятельная работа с раздаточным материалом «*Скрин-шот»* может проводиться вместо работы с конспектом лекций, если композиция каждой страницы материала построена лектором таким образом, что достаточно свободного места для конспектирования

материалов лекции, комментариев и выражения собственных мыслей студента по материалам услышанного или прочитанного.

В случае, когда студенты ведут отдельные конспекты лекций, работа с раздаточным материалом «*Скрин-шот»* проводится вместе с работой с конспектом лекций по каждой теме.

3. В связи с большим объемом изучаемого материала, интересом который он представляет для современного образованного человека, некоторые вопросы выносятся за рамки лекций. Это предусмотрено рабочим учебным планом подготовки специалистов. *Изучение вопросов, выносимых за рамки лекционных занятий* (дискуссионных вопросов раздела 2), предполагает самостоятельное изучение студентами дополнительной литературы и её конспектирование по этим вопросам.

4. В ходе *практических занятий* реализуется этап формирования компетентностной компоненты в части овладения способами деятельности, а также проводится разъяснение теоретических положений курса, уточнения междисциплинарных связей. *Подготовка к практическому занятию* предполагает большую самостоятельную работу и включает в себя:

1) знакомство с планом занятия и подбор материала к нему по указанным источникам (конспект лекции, основная, справочная и дополнительная литература, электронные и Интернет-ресурсы);

2) запоминание подобранного по плану материала;

3) освоение терминов, перечисленных в глоссарии;

4) ответы на вопросы, приведенные к каждой теме;

5) обдумывание вопросов для обсуждения, выдвижение собственных вариантов ответа;

6) выполнение заданий преподавателя;

7) подготовка (выборочно) индивидуальных заданий.

Задания, приведенные в планах занятий, выполняются всеми студентами в обязательном порядке.

Для эффективной реализации целей практических занятий обучающимся рекомендуется регулярно обновлять навыки работы с информационными технологиями: с операционной системой ОС Windows и программным обеспечением персонального компьютера ПО Microsoft Office; с локальной вычислительной сетью (ЛВС) университета и глобальной сетью Интернет; с локальными версиями

СПС Консультант Плюс, Гарант; с другими информационными технологиями.

5. В*ыполнение групповых и индивидуальных домашних заданий* является обязательной формой самостоятельной работы студентов и предполагает подготовку индивидуальных или групповых (на усмотрение преподавателя) *докладов (сообщений, рефератов, эссе, творческих заданий)* на практических занятиях и разработку мультимедийных презентаций к ним.

Доклад – продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

Эссе – средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ проблемы с использованием концепций и аналитического инструментария соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме.

Реферат – продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее, приводит список используемых источников.

Творческое задание – частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения. Может выполняться в индивидуальном порядке или группой обучающихся.

Преподаватель сам формирует задание или студенты имеют возможность самостоятельно выбрать одну из предполагаемых преподавателем тем и выступить на семинарском занятии. Доклад (резюме, эссе и т.д.) как форма самостоятельной учебной деятельности студентов представляет собой рассуждение на определенную тему на основе обзора нескольких источников в целях доказательства или опровержения какого-либо тезиса.

Информация источников используется для аргументации, иллюстрации и т.д. своих мыслей. Цель написания такого рассуждения не дублирование имеющейся литературы на эту тему, а подготовка студентов к проведению собственного научного исследования, к правильному оформлению его описания в соответствии с требованиями.

Работа студентов по подготовке доклада (сообщения, рефератов, эссе, творческих заданий) заключается в следующем:

1) подбор научной литературы по выбранной теме;

2) работа с литературой, отбор информации, которая соответствует теме и помогает доказать тезисы;

3) анализ проблемы, фактов, явлений;

4) систематизация и обобщение данных, формулировка выводов;

5) оценка теоретического и практического значения рассматриваемой проблемы;

6) аргументация своего мнения, оценок, выводов, предложений;

7) выстраивание логики изложения;

8) указание источников информации, авторов излагаемых точек зрения;

9) правильное оформление работы (ссылки, список использованной литературы, рисунки, таблицы) по стандарту.

Самостоятельность студента при подготовке доклада (сообщение, эссе) проявляется в выборе темы, ракурса её рассмотрения, источников для раскрытия темы, тезисов, аргументов для их доказательства, конкретной информации из источников, способа структурирования и обобщения информации, структуры изложения, а также в обосновании выбора темы, в оценке её актуальности, практического и теоретического значения, в выводах.

Выступление с докладом (резюме, эссе) не должно превышать 7-10 минут. После устного выступления автор отвечает на вопросы аудитории (студентов, преподавателя) по теме и содержанию своего выступления.

Цель и задачи данного вида самостоятельной работы студентов определяют требования, предъявляемые к докладу (резюме, эссе), и критерии его оценки:

1) логическая последовательность изложения;

2) аргументированность оценок и выводов, доказанность тезиса;

3) ясность и простота изложения мыслей (отсутствие многословия и излишнего наукообразия);

4) самостоятельность изложения материала источников;

5) корректное указание в тексте доклада источников информации, авторов проводимых точек зрения;

6) стилистическая правильность и выразительность (выбор языковых средств, соответствующих научному стилю речи);

7) уместное использование иллюстративных средств (цитат, сносок, рисунков, таблиц, слайдов).

Изложение материалов доклада может сопровождаться *мультимедийной презентацией*. Разработка мультимедийной презентации выполняется по требованию преподавателя или по желанию студента.

Презентация должна быть выполнена в программе Power Point и включать такое количество слайдов, какое необходимо для иллюстрирования материала доклада в полном объеме.

Основные методические требования, предъявляемые к презентации:

1) логичность представления с согласованность текстового и визуального материала;

2) соответствие содержания презентации выбранной теме и выбранного принципа изложения / рубрикации информации (хронологический, классификационный, функционально-целевой и др.);

3) соразмерность (необходимая и достаточная пропорциональность) текста и визуального ряда на каждом слайде (не менее 50% - 50%, или на 10-20% более в сторону визуального ряда);

4) комфортность восприятия с экрана (цвет фона; размер и четкость шрифта);

5) эстетичность оформления (внутреннее единство используемых шаблонов предъявления информации; упорядоченность и выразительность графических и изобразительных элементов);

6) допускается наличие анимационных и звуковых эффектов.

Оценка доклада (резюме, эссе) производится в рамках 12-балльного творческого рейтинга действующей в ЮЗГУ балльно - рейтинговой оценки успеваемости и качества знаний студентов. Итоговая оценка является суммой баллов, выставляемых преподавателем с учетом мнения других студентов по каждому из перечисленных выше методических требований к докладу и презентации.

Формой самостоятельной работы студентов также является *выполнение практических заданий (решения задач, выполнения расчетных работ, оформление отчетов о самостоятельной работе*), содержание которых определяется содержанием настоящих методических указаний. Часть практических заданий может быть выполнена студентами на аудиторных практических (лабораторных) занятиях под руководством преподавателя. После того, как преподавателем объявлено, что рассмотрение данной темы на аудиторных занятиях завершено, студент переходит к самостоятельному выполнению практических заданий, пользуясь настоящими методическими указаниями, конспектом лекций по соответствующей теме, записями, сделанными на практических занятиях, дополнительной литературой по теме. Все практические задания для самостоятельного выполнения студентами, приведенные в настоящих методических указаниях обязательны для выполнения в полном объеме.

6. Подготовка к тестированию предусматривает повторение лекционного материала и основных терминов, а также самостоятельное выполнение заданий в текстовой форме, приведенных в настоящих методических указаниях.

7. *Самоконтроль* является обязательным элементом самостоятельной работы студента. Он позволяет формировать умения самостоятельно контролировать и адекватно оценивать результаты своей учебной деятельности и на этой основе управлять процессом овладения знаниями. Овладение умениями самоконтроля формирует навыки планирования учебного труда, способствует углублению внимания, памяти и выступает как важный фактор развития познавательных способностей.

Самоконтроль включает:

1) ответ на вопросы для самоконтроля для самоанализа глубины и прочности знаний и умений по дисциплине;

2) критическую оценку результатов своей познавательной деятельности.

Самоконтроль учит ценить свое время, позволяет вовремя заменить и исправлять свои ошибки.

Формы самоконтроля могут быть следующими:

1) устный пересказ текста лекции и сравнение его с содержанием конспекта лекции;

2) ответ на вопросы, приведенные к каждой теме (см. раздел 2 настоящих методических указаний);

3) составление плана, тезисов, формулировок ключевых положений текста по памяти;

4) ответы на вопросы и выполнение заданий для самопроверки (настоящие методические указания предполагают вопросы для самоконтроля по каждой изучаемой теме);

5) самостоятельное тестирование по предложенным в настоящих методических указаниях тестовых заданий.

Самоконтроль учебной деятельности позволяет студенту оценивать эффективность и рациональность применяемых методов и форм умственного труда, находить допускаемые недочеты и на этой основе проводить необходимую коррекцию своей познавательной деятельности.

Обучающиеся осуществляют самоконтроль результатов самостоятельной работы по тем же критериям и показателям, которые определяются преподавателем для проведения внешнего контроля. Это позволяет студенту объективно оценить не только результаты обучения, но и уровень сформированности соответствующих компетенций и развития личностных психологических качеств, важных для профессиональной деятельности будущего юриста.

При возникновении сложностей по усвоению программного материала необходимо посещать консультации по дисциплине, задавать уточняющие вопросы на лекциях и практических занятиях, уделять время самостоятельной подготовке (часы на самостоятельное изучение), осуществлять все формы самоконтроля.

1.4. Формы контроля знаний

1.4.1. Текущий контроль изучения дисциплины

Текущий контроль изучения дисциплины осуществляется на основе балльно-рейтинговой системы (БРС) контроля оценки знаний. В процессе освоения дисциплины студенты должны пройти четыре точки контроля знаний.

Студент на каждой контрольной точке может получить максимально 16 баллов (из них: 4 балла – за посещаемость, 12 баллов – за успеваемость). Таким образом, 100% результат освоения дисциплины за четыре точки контроля знаний выглядит следующим образом: 48 баллов – максимальный за успеваемость; 16 баллов – максимальный результат за посещаемость; 36 баллов – максимальный результат за итоговый контроль (за зачёт) по дисциплине осуществляются следующим образом.

Для текущего контроля в четырех контрольных точках по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий критерий выполнения заданий практического занятия (таблица 2):

- доля правильных ответов менее 50% – минимальный балл;
- доля правильных ответов более 50% – максимальный балл.

Таблица 2 – Контроль изучения дисциплины

Форма контроля	Минимальный балл	Максимальный балл
1 контрольная точка		
Практическое занятие №1. Поиск и систематизация информации на тему «ИБ и ее составные части». Разработка текстового документа и его презентация	2	4
Практическое занятие №2. Поиск и систематизация информации на тему «Актуальность и важность проблемы обеспечения ИБ». Разработка текстового документа и его презентация	2	4
Практическое занятие №3. Поиск и систематизация информации на тему «Основные угрозы информационной безопасности». Разработка текстового документа и его презентация	2	4
Итого за 1 контрольную точку	6	12

2 контрольная точка		
Практическое занятие №4. Поиск и систематизация информации на тему «Правовое обеспечение информационной безопасности». Разработка текстового документа и его презентация	3	6
Практическое занятие №5. Поиск и систематизация информации на тему «Организационное обеспечение информационной безопасности». Разработка текстового документа и его презентация	3	6
Итого за 2 контрольную точку	6	12
3 контрольная точка		
Практическое занятие №6. Поиск и систематизация информации на тему «Защита информации в компьютерных системах от случайных угроз и традиционного шпионажа». Разработка текстового документа и его презентация	3	6
Практическое занятие №7. Поиск и систематизация информации на тему «Методы и средства защиты информации от несанкционированного доступа и изменения структур в компьютерных системах». Разработка текстового документа и его	3	6
Итого за 3 контрольную точку	6	12
4 контрольная точка		
Практическое занятие №8. Поиск и систематизация информации на тему «Защита информации в распределенных компьютерных системах». Разработка текстового документа и его презентация	3	6
Практическое занятие №9. Поиск и систематизация информации на тему «Защита компьютерных систем от вирусов и вредоносных программ». Разработка текстового документа и его презентация	3	6
Итого за 4 контрольную точку	6	12
Итоговое количество баллов (за контрольные точки, не включая посещаемость)	24	48
Форма контроля– зачет		36

1.4.2. Итоговый (промежуточный) контроль

Учебным планом специальности 40.05.02 Правоохранительная деятельность предусмотрена промежуточная аттестация по дисци-

плине «Основы информационной безопасности» в форме зачёта в четвёртом семестре обучения.

Оценивание знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, осуществляется в соответствии с положением «О проведении текущего контроля успеваемости и промежуточной аттестации студентов в ЮЗГУ (П 02.034-2014)».

Зачет проводится в компьютерном классе в соответствии с утвержденным расписанием в зачетную неделю до экзаменационной сессии и принимается преподавателем, ведущем практические (семинарские) занятия в группе, или читающем лекции по данному курсу. Форма проведения зачета устанавливается кафедрой как устное собеседование или тестирование с использованием компьютерной контролирующей программы.

Если к моменту проведения зачёта студент не имеет задолженностей по контролируемым темам и набирает 50 и более баллов, они могут быть выставлены ему в виде поощрения в ведомость и в зачетную книжку без процедур опроса или принятия зачёта. По желанию студента он может добрать баллы на зачете, проводимом в виде собеседования по теоретическому материалу данной дисциплины в объеме перечня вопросов, приведенного в **приложении А**. При этом количество баллов, набираемых на зачете, не должно превышать 36, а итоговая сумма 100. Право выбора вопроса или тестового задания предоставляется преподавателю, проводящему собеседование.

Промежуточную аттестацию студенты заочной формы обучения проходят с использованием тестовых технологий. Тестовые задания для проведения зачёта приведены в **Приложении Б**.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Тема 1. Введение в дисциплину «Основы информационной безопасности»

Структура (план)

1. Цели, задачи, структура, содержание, формируемые компетенции и процедура проведения текущего контроля.
2. Информационная безопасность и ее составные части.
3. Понятия целостности, конфиденциальности, аутентичности и доступности информации.
4. Защищенность информационных ресурсов, систем и технологий.

Глоссарий

В настоящее время *систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере* представляет Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

Информационная сфера – совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Национальные интересы в информационной сфере– объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы.

Угроза информационной безопасности (информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Информационная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних

информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Силы обеспечения информационной безопасности – государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

Средства обеспечения информационной безопасности – правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности.

Система обеспечения информационной безопасности – совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов

Информационные продукты (продукция) – документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей.

Информационные услуги – действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами.

Доступность информации – возможность реализации беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Аутентичность (authenticity) – свойство, гарантирующее, что субъект или ресурс идентичны заявленным. Аутентичность применяется к таким субъектам, как пользователи, к процессам, системам и информации.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Объект защиты информации – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Практическое занятие №1

Тема: «Поиск и систематизация информации на тему «Информационная безопасность и ее составные части». Разработка текстового документа и его презентация»

Суть практического занятия: Оценка уровней сформированности компетенций в категориях УМЕТЬ, ВЛАДЕТЬ по результатам выполнения заданий с использованием возможностей компьютерных технологий для поиска информации на заданную тему и оформления рефератов-презентаций.

Самостоятельная работа

Кейс-задача №1. Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов:

1. Современные нормативные правовые акты РФ, регламентирующие информационную безопасность страны.

2. Понятие информационной безопасности и ее составных частей в современных НПАРФ.

3. Понятия целостности, конфиденциальности, аутентичности и доступности информации в современных НПА РФ.

4.Понятия защищенности информационных ресурсов, информационных систем и информационных технологий в современных НПА РФ.

Методика выполнения:

Алгоритм структурирования учебного материала.

1. Включить персональный компьютер, войти в работу с СПС КонсультантПлюс (Гарант) или сеть Интернета, найти в базе данных соответствующую теме информацию в текстах современных НПА, скопировать её на отдельный файл в текстовом редакторе WORD и оформить в виде Тезауруса в соответствии с требованиями к оформлению текстовых документов.

2. Выполнить структурно-логический анализ отобранного учебного материала: выделить по тексту (цветом, фоном) главное содержание (ядро), основные положения, понятия и определения по теме реферата-презентации.

3. Построить структурно-логическую схему учебной информации (план презентации).

4. Расположить учебный материал с учетом логики формирования учебных понятий, лишний текст удалить.

5. Выполнить подбор опорных сигналов (ключевых слов,

символов, фрагментов схем) и их кодировку (при необходимости).

6. Выполнить компоновку учебного материала в блоки (содержание слайдов) и составить первичный вариант (макет) презентации.

7. Критически осмыслить первичный вариант, при необходимости перекомпоновать, перестроить, упростить отобранный учебный материал.

Алгоритм создания реферата-презентации.

Приветствуются любые другие алгоритмы создания презентаций в пределах возможностей графического редактора Power Point и других офисных программ.

1. На титульном слайде разместить: название учебного заведения, кафедры, учебной дисциплины, вид работы (реферат-презентация), название темы, реквизиты автора, место (г. Курск) и год. Размеры и цвета шрифта выбирать в соответствии с правилами визуализации.

2. Аналогичным образом создать макет второго слайда – плана реферата-презентации и разместить на нем путем копирования из структурированного текста необходимую информацию.

3. Соблюдая общие рекомендации, правила компоновки объектов на слайде и основные правила использования цвета (**Приложение В**) создать не менее десяти слайдов по теме презентации, копируя необходимый структурированный учебный материал из файла.

Вопросы для самоконтроля

1. Назовите современные нормативные правовые акты РФ, регламентирующие информационную безопасность страны.

2. Раскройте понятие информационной безопасности и ее составных частей в современных нормативных правовых актах РФ.

3. Раскройте понятия целостности информации в современных нормативных правовых актах РФ.

4. Раскройте понятия конфиденциальности информации в современных нормативных правовых актах РФ.

5. Раскройте понятия аутентичности информации в современных нормативных правовых актах РФ.

6. Раскройте понятия доступности информации в современных нормативных правовых актах РФ.

7. Раскройте понятия защищенности информационных ресурсов в современных нормативных правовых актах РФ.

8. Раскройте понятия защищенности информационных систем в современных нормативных правовых актах РФ.

9. Раскройте понятия защищенности информационных технологий в современных нормативных правовых актах РФ.

10. Раскройте сущность основных положений новой доктрины информационной безопасности РФ в контексте профессиональной деятельности юриста.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

4. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

6. Указ Президента РФ от 31.12.2015 №683 «О стратегии национальной безопасности Российской Федерации».

7. Указ Президента РФ от 05.12.2016 №646 «О доктрине информационной безопасности Российской Федерации.

8. Указ Президента РФ от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».

9. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. – Старый Оскол : ТНТ, 2013. – 384 с.

10. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

2.2. Тема 2. Сущность проблемы информационной безопасности (ИБ)

Структура (план)

1. Актуальность и важность проблемы обеспечения информационной безопасности.
2. Предпосылки, направления и перспективы киберпреступности.
3. Основные понятия в области информационной безопасности.
4. Аспекты информационной безопасности: доступность, целостность, конфиденциальность.

Глоссарий

Критическая информационная инфраструктура – совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой.

Объекты критической информационной инфраструктуры – информационные системы и информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, в сфере здравоохранения, транспорта, связи, в кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг.

Экосистема цифровой экономики – партнерство организаций, обеспечивающее постоянное взаимодействие принадлежащих им

технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан.

Согласно Конвенции Совета Европы о киберпреступности (Будапешт, 2001), *киберпреступления* – это правонарушения, направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и данных, а также неправомерное использование указанных систем, сетей и данных.

Следовательно, *киберпреступления* – это правонарушения экономического, политического и социального характера, выражающиеся в форме совершения незаконных деяний (действий, бездействия) во всех сферах общественной жизнедеятельности с помощью сети Интернет, иных средств электронной коммуникации.

Информационным оружием называются средства: уничтожения, искажения или хищения информационных массивов; преодоления систем защиты; ограничения допуска законных пользователей; дезорганизация работы технических средств, компьютерных систем.

Атакующим информационным оружием сегодня можно назвать:

– *компьютерные вирусы,* способные размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.д.;

– *логические бомбы* – программные закладные устройства, которые заранее внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;

– *средства подавления информационного обмена* в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления;

– *различного рода ошибки*, сознательно вводимые противником в программное обеспечение объекта.

Политическая разведка – это деятельность, направленная на добывание сведений внутренней и внешней политики разведстраны; деятельность, направленная на свершение акций по подрыву политических устоев государства.

Экономическая разведка – это вид внешней разведки, объекта-

ми которой являются промышленность, транспорт, торговля, финансовые и денежно-кредитные системы, природные ресурсы и т.п.

Военная разведка – это вид разведки, объектами которой являются научно-исследовательские центры, научно-технические учреждения, видные ученые, специалисты, составляющие научно-технический потенциал страны.

Основные формы разведдеятельности иностранных спецслужб:

1) агентурная разведка;

2) легальная разведка;

3) техническая разведка;

4) аналитическая обработка первичной информации.

Агентурная разведка использует для добывания информации и свершения диверсионных акций специально подобранных, завербованных и тщательно подготовленных агентов из числа граждан разведстраны или иностранцев.

Легальная разведка – деятельность иностранных спецслужб, используемая для получения информации при различных связях и контактах с нашей страной, не прибегая при этом к тайным операциям, не скрывая источников информации.

Основные формы легальной разведки:

1) приобретение и анализ всех открытых публикаций, которые издаются в разведстране;

2) получение информации при непосредственных контактах агентов спецслужб с интересующими их лицами на различного рода приемах, встречах, конференциях;

3) визуальное наблюдение, кино- и фотосъемка при перемещении иностранцев по стране.

Техническая разведка – это сбор информации с использованием технических средств.

Аналитическая обработка первичной информации – это получение разведоценок более высокого уровня при анализе первичной развединформации с использованием вычислительной техники и специально разработанных программ обработки.

Основные составляющие информационной безопасности сформулированы в Европейских критериях, принятых ведущими странами Европы. В качестве *стандартной модели информационной*

безопасности часто приводят модель из трёх категорий:

1) конфиденциальность (англ. confidentiality) – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право или обеспечение доступа к информации только авторизованному кругу субъектов;

2) целостность (англ. integrity) – избежание несанкционированной модификации информации и обеспечение существования информации в неискаженном виде;

3) доступность (англ. availability) – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа и обеспечение готовности системы к обслуживанию поступающих к ней запросов.

Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации. Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, *нарушение доступности* приводит к отказу в доступе к информации, *нарушение целостности* приводит к фальсификации информации и, наконец, *нарушение конфиденциальности* приводит к раскрытию информации.

Классификацию мер защиты можно представить в виде трех уровней:

Законодательный уровень. В Уголовном кодексе РФ имеется глава 28. Преступления в сфере компьютерной информации. Она содержит три следующих статьи: статья 272. Неправомерный доступ к компьютерной информации; статья 273. Создание, использование и распространение вредоносных программ для ЭВМ; статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Административный и процедурный уровни. На административном и процедурном уровнях формируются политика безопасности и комплекс процедур, определяющих действия персонала в штатных и критических ситуациях. Этот уровень зафиксирован в руководящих документах, выпущенных Гостехкомиссией РФ и ФАПСИ.

Программно-технический уровень. К этому уровню относятся программные и аппаратные средства, которые составляют технику информационной безопасности. К ним относятся и идентификация пользователей, и управление доступом, и криптография, и экрани-

рование, и многое другое.

Практическое занятие №2

Тема: «Поиск и систематизация информации на тему «Актуальность и важность проблемы обеспечения информационной безопасности». Разработка текстового документа и его презентация»

Суть практического занятия: Оценка уровней сформированности компетенций в категориях УМЕТЬ, ВЛАДЕТЬ по результатам выполнения заданий с использованием возможностей компьютерных технологий для поиска информации на заданную тему и оформления рефератов-презентаций.

Самостоятельная работа

Кейс-задача. Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов:

1. Актуальность и важность проблемы обеспечения информационной безопасности.
2. Предпосылки, направления и перспективы киберпреступности в современной информационной среде.
3. Основные понятия в области информационной безопасности.
4. Аспекты информационной безопасности: доступность, целостность, конфиденциальность.

Методика выполнения:

Алгоритм структурирования учебного материала.

1. Включить персональный компьютер, войти в работу с СПС КонсультантПлюс (Гарант) или сеть Интернета, найти в базе данных соответствующую теме информацию в текстах современных НПА, скопировать её на отдельный файл в текстовом редакторе WORD и оформить в виде Тезауруса в соответствии с требованиями к оформлению текстовых документов.
2. Выполнить структурно-логический анализ отобранного учебного материала: выделить по тексту (цветом, фоном) главное содержание (ядро), основные положения, понятия и определения по теме реферата-презентации.
3. Построить структурно-логическую схему учебной

информации (план презентации).

4. Расположить учебный материал с учетом логики формирования учебных понятий, лишний текст удалить.

5. Выполнить подбор опорных сигналов (ключевых слов, символов, фрагментов схем) и их кодировку (при необходимости).

6. Выполнить компоновку учебного материала в блоки (содержание слайдов) и составить первичный вариант (макет) презентации.

7. Критически осмыслить первичный вариант, при необходимости перекомпоновать, перестроить, упростить отобранный учебный материал.

Алгоритм создания реферата-презентации.

Приветствуются любые другие алгоритмы создания презентаций в пределах возможностей графического редактора Power Point и других офисных программ.

1. На титульном слайде разместить: название учебного заведения, кафедры, учебной дисциплины, вид работы (реферат-презентация), название темы, реквизиты автора, место (г. Курск) и год. Размеры и цвета шрифта выбирать в соответствии с правилами визуализации.

2. Аналогичным образом создать макет второго слайда – плана реферата-презентации и разместить на нем путем копирования из структурированного текста необходимую информацию.

3. Соблюдая общие рекомендации, правила компоновки объектов на слайде и основные правила использования цвета (**Приложение В**) создать не менее десяти слайдов по теме презентации, копируя необходимый структурированный учебный материал из файла.

Вопросы для самоконтроля

1. Раскройте актуальность и важность проблемы обеспечения информационной безопасности.

2. Раскройте понятие «критическая информационная инфраструктура» и её объектов как целей информационных угроз.

3. Раскройте сущность понятия «киберпреступления».

4. Предпосылки, направления и перспективы киберпреступности в современной информационной среде.

5. Дайте определение термина «информационное оружие».

6. Что сегодня называют «атакующим информационным оружием»?

7. На что направлена деятельность политической, экономической и военной разведок иностранных государств.

8. Назовите основные формы разведдеятельности иностранных спецслужб.

9. Раскройте сущность основных составляющих информационной безопасности: конфиденциальности, целостности и доступности информации.

10. Раскройте содержание законодательного, административно-процедурного и программно-технического уровней обеспечения информационной безопасности.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

4. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

6. Указ Президента РФ от 31.12.2015 №683 «О стратегии национальной безопасности Российской Федерации».

7. Указ Президента РФ от 05.12.2016 №646 «О доктрине информационной безопасности Российской Федерации.

8. Указ Президента РФ от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».

9. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. – Старый Оскол : ТНТ, 2013. – 384 с.

10. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

2.3. Тема 3. Основные угрозы информационной безопасности

Структура (план)

1. Понятие угрозы информационной безопасности.
2. Характеристики информационного ресурса как объекта защиты.
3. Классификация и характеристика угроз информационной безопасности.
4. Угрозы случайные и преднамеренные, внешние и внутренние, стихийного и искусственного характера.
5. Проявления, последствия и основные способы реализации угроз.

Глоссарий

Угроза информационной безопасности (информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Информация об угрозе безопасности объекта государственной охраны – сведения об условиях и факторах, создающих опасность для жизни и здоровья лица, подлежащего государственной охране, иным охраняемым законом его жизненно важным интересам, или о возможных посягательствах физического, морального или иного характера, или нанесения данному лицу и охраняемым законом его жизненно важным интересам иного ущерба.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Информационный терроризм – использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях.

Новые информационные угрозы порождаются *расширением областей применения информационных технологий* как фактора развития экономики и совершенствования функционирования

общественных и государственных институтов и *использованием возможностей трансграничного оборота информации* для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

Угрозы информационной безопасности военно-промышленного комплекса – обусловлены наращиванием рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях с одновременным усилением деятельности организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

Угрозы информационной безопасности внутриполитической и социальной ситуации – обусловлены расширяющимися масштабами использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий. Наращивание информационного воздействия на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

Угрозы информационной безопасности объектов критической информационной инфраструктуры – обусловлены широким использованием различными террористическими и экстремистскими организациями механизмов информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также

привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

Угрозы информационной безопасности в сфере правопорядка – обусловлены возрастающими масштабами компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

Угрозы информационной безопасности в области обороны – обусловлены увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности негативно влияет на состояние информационной безопасности в области обороны страны.

Угрозы информационной безопасности в области государственной и общественной безопасности – обусловлены постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

Угрозы информационной безопасности в экономической сфере – обусловлены недостаточным уровнем развития

конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

Угрозы информационной безопасности в области науки, технологий и образования – обусловлены недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы.

Угрозы информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства – обусловлены стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве. Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.

Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической

стабильности и равноправного стратегического партнерства.

Классификация угроз безопасности информации:

а) угрозы конфиденциальности информации – в соответствии с требованиями федеральных законов обязательность соблюдения конфиденциальности касается только информации ограниченного доступа, к которой относится информация, представляющая государственную тайну, а также конфиденциальная информация (сведения, составляющие коммерческую, банковскую, служебную, профессиональную тайну, содержащие персональные данные и т.д.). Разглашение сведений ограниченного доступа может произойти как преднамеренно (при прямом умысле), так и непреднамеренно (по неосторожности).

К угрозам, *создающим опасность конфиденциальности информации*, относится утечка информации, под которой понимается неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к ней или получения защищаемой информации иностранными разведками и другими заинтересованными субъектами (заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо)

б) угрозы целостности и доступности информации – сюда относятся факторы (явление, действие или процесс), результатом которых могут быть неправомерное уничтожение или неправомерное модифицирование (искажение, подмена) информации, а к угрозам доступности информации - факторы, результатом которых может быть неправомерное блокирование доступа к информации. Угрозы целостности и доступности информации можно разделить на преднамеренные и непреднамеренные

Несанкционированное предоставление информации – противоправное предание огласке сведений ограниченного доступа, при котором они стали достоянием определённого круга посторонних лиц.

Несанкционированное распространение информации – противоправное предание огласке сведений ограниченного доступа, при котором они стали достоянием неопределённого круга

посторонних лиц.

Перехват информации – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов, то есть сигналов, по параметрам которых может быть определена защищаемая информация.

Утечка информации – неконтролируемое распространение защищаемой информации.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уничтожение информации (destruction of information) – любое условие, делающее информацию непригодной для использования независимо от причины.

Практическое занятие №3

Тема: «Поиск и систематизация информации на тему «Основные угрозы информационной безопасности». Разработка текстового документа и его презентация»

Суть практического занятия: Оценка уровней сформированности компетенций в категориях УМЕТЬ, ВЛАДЕТЬ по результатам выполнения заданий с использованием возможностей компьютерных технологий для поиска информации на заданную тему и оформления рефератов-презентаций.

Самостоятельная работа

Кейс-задача. Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов:

1. Понятие угрозы информационной безопасности.
2. Характеристики информационного ресурса как объекта защиты.
3. Классификация и характеристика угроз информационной безопасности.
4. Угрозы случайные и преднамеренные, внешние и

внутренние, стихийного и искусственного характера.

5. Проявления, последствия и основные способы реализации угроз.

Методика выполнения:

Алгоритм структурирования учебного материала.

1. Включить персональный компьютер, войти в работу с СПС КонсультантПлюс (Гарант) или сеть Интернета, найти в базе данных соответствующую теме информацию в текстах современных НПА, скопировать её на отдельный файл в текстовом редакторе WORD и оформить в виде Тезауруса в соответствии с требованиями к оформлению текстовых документов.

2. Выполнить структурно-логический анализ отобранного учебного материала: выделить по тексту (цветом, фоном) главное содержание (ядро), основные положения, понятия и определения по теме реферата-презентации.

3. Построить структурно-логическую схему учебной информации (план презентации).

4. Расположить учебный материал с учетом логики формирования учебных понятий, лишний текст удалить.

5. Выполнить подбор опорных сигналов (ключевых слов, символов, фрагментов схем) и их кодировку (при необходимости).

6. Выполнить компоновку учебного материала в блоки (содержание слайдов) и составить первичный вариант (макет) презентации.

7. Критически осмыслить первичный вариант, при необходимости перекомпоновать, перестроить, упростить отобранный учебный материал.

Алгоритм создания реферата-презентации.

Приветствуются любые другие алгоритмы создания презентаций в пределах возможностей графического редактора Power Point и других офисных программ.

1. На титульном слайде разместить: название учебного заведения, кафедры, учебной дисциплины, вид работы (реферат-презентация), название темы, реквизиты автора, место (г. Курск) и год. Размеры и цвета шрифта выбирать в соответствии с правилами визуализации.

2. Аналогичным образом создать макет второго слайда – плана

реферата-презентации и разместить на нем путем копирования из структурированного текста необходимую информацию.

3. Соблюдая общие рекомендации, правила компоновки объектов на слайде и основные правила использования цвета (**Приложение В**) создать не менее десяти слайдов по теме презентации, копируя необходимый структурированный учебный материал из файла.

Вопросы для самоконтроля

1. Раскройте понятие угрозы информационной безопасности.
2. Дайте характеристику информационного ресурса как объекта защиты.
3. Охарактеризуйте основные виды информационных угроз в контексте профессиональной деятельности юриста.
4. Раскройте характеристики угроз конфиденциальности, целостности и доступности информации.
5. Раскройте сущность угроз информационной безопасности страны в контексте информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации.
6. Раскройте сущность угроз информационной безопасности страны в контексте роста масштабов компьютерной преступности и информационного воздействия международных террористических и экстремистских организаций.
7. Раскройте сущность угроз информационной безопасности страны в контексте увеличения масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях.
8. Раскройте сущность угроз информационной безопасности страны в области государственной и общественной безопасности.
9. Раскройте сущность угроз информационной безопасности страны в области экономики, науки, технологий и образования.
10. Раскройте сущность угроз информационной безопасности страны в области стратегической стабильности и равноправного стратегического партнерства.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

4. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

6. Указ Президента РФ от 31.12.2015 №683 «О стратегии национальной безопасности Российской Федерации».

7. Указ Президента РФ от 05.12.2016 №646 «О доктрине информационной безопасности Российской Федерации.

8. Указ Президента РФ от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».

9. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. – Старый Оскол : ТНТ, 2013. – 384 с.

10. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

2.4. Тема 4. Правовое обеспечение информационной безопасности

Структура (план)

1. Понятие правового обеспечения ИБ.
2. Особенности информации как объекта права.
3. Государственная политика РФ в области правового обеспечения.
4. Уровни правового регулирования в сфере ИБ.
5. Основные конституционные и правовые нормы в области ИБ.
6. Понятия банковской, коммерческой и служебной тайны.
7. Наказания за преступления в сфере компьютерной информации.
8. Зарубежное законодательство в области ИБ.

Глоссарий

Право на информацию – право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Правовая защита информации – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Правовой режим информационных ресурсов – нормы, устанавливающие порядок документирования информации, право собственности на нее, категорию информации по уровню доступа к ней и порядок правовой защиты информации.

Правовой режим конфиденциальности информации – это правовой режим доступа к конфиденциальной информации, а также регламентация порядка ее использования, способов и средств обеспечения ее защиты.

Правовой режим секретности информации – это правовой режим доступа к секретной информации, а также регламентация ее использования, способов и средств обеспечения ее защиты.

Сведения особой важности – сведения в области военной, внешнеполитической, экономической, научно-технической, разве-

дывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

Сведения, составляющие государственную тайну – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Секретные сведения – все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности.

Совершенно секретные сведения – сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

Единая система идентификации и аутентификации – федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах.

Информация ограниченного доступа – информация, доступ к которой ограничен в интересах обеспечения национальной безопасности в соответствии с законодательством о государственных секретах и иными нормативно-правовыми актами, регулирующими отношения в области защиты государственных секретов.

Служебная информация ограниченного доступа – несекретная информация, касающаяся деятельности организации, ограничение на распространение которой диктуется служебной необходимостью. Такая информация может включать в себя все виды конфиденци-

альной информации, являющейся собственностью юридического лица, кроме информации, составляющей государственную тайну. В ряде случаев на документах, содержащих такую информацию, может стоять пометка «Для служебного пользования».

Информация ограниченного пользования – это творческая информация, на которую распространяется авторское право и право на интеллектуальную собственность, несанкционированное использование которой наносит вред авторам этой информации.

Статистическая информация (данные) – любая информация, которая в количественном и качественном измерении характеризует массовые явления и процессы, имеющие место в экономической, социальной и других сферах общественной жизни

Информация, составляющая коммерческую тайну – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны

Экспертиза документа по защите информации – рассмотрение документа по защите информации физическим или юридическим лицом, имеющим право на проведение работ в данной области, с целью подготовить соответствующее экспертное заключение.

Примечание – Экспертиза документа по защите информации может включать в себя научно-техническую, правовую, метрологическую, патентную и терминологическую экспертизу.

Электронная подпись – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа.

Эффективность защиты информации – степень соответствия результатов защиты информации цели защиты информации.

Коммерческая тайна – охраняемое законом право предприятия на засекречивание (ограниченный доступ) производственных,

технологических, торговых финансовых и других хозяйственных операций и документации по ним.

Профессиональная тайна – общее название группы охраняемых законом тайн, необходимость соблюдения которых вытекает из доверительного характера отдельных профессий

Служебная тайна – сведения о сферах деятельности государственных органов, доступ к которым ограничивается служебной необходимостью и разглашение или утрата которых может нанести ущерб государственным органам или государству.

Персональные данные – информация, с помощью которой можно идентифицировать человека: ФИО, место и год рождения, адрес прописки, паспортные данные и т.д.

Личная тайна – сведения конфиденциального характера, разглашение которых может нанести материальный ущерб отдельному (физическому) лицу.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение.

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

Наказания за преступления в сфере компьютерной информации – определены Уголовным кодексом РФ в главе 28. Преступления в сфере компьютерной информации. Она содержит три следующих статьи: статья 272. Неправомерный доступ к компьютерной информации; статья 273. Создание, использование и распространение вредоносных программ для ЭВМ; статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Практическое занятие №4

Тема: «Поиск и систематизация информации на тему «Правовое обеспечение информационной безопасности». Разработка текстового документа и его презентация»

Суть практического занятия: Оценка уровней

сформированности компетенций в категориях УМЕТЬ, ВЛАДЕТЬ по результатам выполнения заданий с использованием возможностей компьютерных технологий для поиска информации на заданную тему и оформления рефератов-презентаций.

Самостоятельная работа

Кейс-задача. Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов:

1. Понятие правового обеспечения информационной безопасности.
2. Особенности информации как объекта права.
3. Государственная политика РФ в области правового обеспечения.
4. Уровни правового регулирования в сфере информационной безопасности.
5. Основные конституционные и правовые нормы в области информационной безопасности.
6. Понятия банковской, коммерческой и служебной тайны.
7. Наказания за преступления в сфере компьютерной информации.
8. Зарубежное законодательство в области информационной безопасности.

Методика выполнения:

Алгоритм структурирования учебного материала.

1. Включить персональный компьютер, войти в работу с СПС КонсультантПлюс (Гарант) или сеть Интернета, найти в базе данных соответствующую теме информацию в текстах современных НПА, скопировать её на отдельный файл в текстовом редакторе WORD и оформить в виде Тезауруса в соответствии с требованиями к оформлению текстовых документов.
2. Выполнить структурно-логический анализ отобранного учебного материала: выделить по тексту (цветом, фоном) главное содержание (ядро), основные положения, понятия и определения по теме реферата-презентации.
3. Построить структурно-логическую схему учебной информации (план презентации).

4. Расположить учебный материал с учетом логики формирования учебных понятий, лишний текст удалить.

5. Выполнить подбор опорных сигналов (ключевых слов, символов, фрагментов схем) и их кодировку (при необходимости).

6. Выполнить компоновку учебного материала в блоки (содержание слайдов) и составить первичный вариант (макет) презентации.

7. Критически осмыслить первичный вариант, при необходимости перекомпоновать, перестроить, упростить отобранный учебный материал.

Алгоритм создания реферата-презентации.

Приветствуются любые другие алгоритмы создания презентаций в пределах возможностей графического редактора Power Point и других офисных программ.

1. На титульном слайде разместить: название учебного заведения, кафедры, учебной дисциплины, вид работы (реферат-презентация), название темы, реквизиты автора, место (г. Курск) и год. Размеры и цвета шрифта выбирать в соответствии с правилами визуализации.

2. Аналогичным образом создать макет второго слайда – плана реферата-презентации и разместить на нем путем копирования из структурированного текста необходимую информацию.

3. Соблюдая общие рекомендации, правила компоновки объектов на слайде и основные правила использования цвета (**Приложение В**) создать не менее десяти слайдов по теме презентации, копируя необходимый структурированный учебный материал из файла.

Вопросы для самоконтроля

1. Раскройте особенности информации как объекта права.

2. Раскройте понятие «Правая защита информации».

3. Раскройте сущность правовых режимов информационных ресурсов, конфиденциальности и секретности информации.

4. Дайте характеристику уровней правового регулирования в сфере информационной безопасности.

5. Назовите основные конституционные и правовые нормы в области информационной безопасности.

6. Раскройте понятия и назовите отличия сведений секретных,

совершенно секретных и особой важности.

7. Раскройте понятия и назовите отличия информации ограниченного доступа, служебной информации ограниченного доступа и информации ограниченного пользования.

8. Раскройте понятия информации, составляющей банковскую, коммерческую и служебную тайны.

9. Какие наказания за преступления в сфере компьютерной информации предусмотрены действующим законодательством?

10. Что такое «Единая система идентификации и аутентификации» и кто определяет порядок её использования?

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

4. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

6. Указ Президента РФ от 31.12.2015 №683 «О стратегии национальной безопасности Российской Федерации».

7. Указ Президента РФ от 05.12.2016 №646 «О доктрине информационной безопасности Российской Федерации.

8. Указ Президента РФ от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».

9. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. – Старый Оскол : ТНТ, 2013. – 384 с.

10. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

2.5. Тема 5. Организационное обеспечение информационной безопасности

Структура (план)

1. Понятие организационного обеспечения ИБ.
2. Характеристика организационных методов обеспечения ИБ.
3. Структура государственных органов РФ, осуществляющих правотворчество и правоприменение в области ИБ.
4. Организационно-распорядительные документы, связанные с защитой сведений конфиденциального характера.
5. Концепция построения комплексной системы обеспечения ИБ и защиты информации.

Глоссарий

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской

Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной

безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

а) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

г) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

б) совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их

готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

Организационная защита информации – составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Практическое занятие №5

Тема: «Поиск и систематизация информации на тему «Организационное обеспечение информационной безопасности». Разработка текстового документа и его презентация»

Суть практического занятия: Оценка уровней сформированности компетенций в категориях УМЕТЬ, ВЛАДЕТЬ по результатам выполнения заданий с использованием возможностей компьютерных технологий для поиска информации на заданную тему и оформления рефератов-презентаций.

Самостоятельная работа

Кейс-задача. Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов:

1. Понятие организационного обеспечения информационной безопасности.
2. Характеристика организационных методов обеспечения информационной безопасности.
3. Структура государственных органов РФ, осуществляющих правотворчество и правоприменение в области информационной безопасности.

4. Организационно-распорядительные документы, связанные с защитой сведений конфиденциального характера.

5. Концепция построения комплексной системы обеспечения информационной безопасности и защиты информации.

Методика выполнения:

Алгоритм структурирования учебного материала.

1. Включить персональный компьютер, войти в работу с СПС КонсультантПлюс (Гарант) или сеть Интернета, найти в базе данных соответствующую теме информацию в текстах современных НПА, скопировать её на отдельный файл в текстовом редакторе WORD и оформить в виде Тезауруса в соответствии с требованиями к оформлению текстовых документов.

2. Выполнить структурно-логический анализ отобранного учебного материала: выделить по тексту (цветом, фоном) главное содержание (ядро), основные положения, понятия и определения по теме реферата-презентации.

3. Построить структурно-логическую схему учебной информации (план презентации).

4. Расположить учебный материал с учетом логики формирования учебных понятий, лишний текст удалить.

5. Выполнить подбор опорных сигналов (ключевых слов, символов, фрагментов схем) и их кодировку (при необходимости).

6. Выполнить компоновку учебного материала в блоки (содержание слайдов) и составить первичный вариант (макет) презентации.

7. Критически осмыслить первичный вариант, при необходимости перекомпоновать, перестроить, упростить отобранный учебный материал.

Алгоритм создания реферата-презентации.

Приветствуются любые другие алгоритмы создания презентаций в пределах возможностей графического редактора Power Point и других офисных программ.

1. На титульном слайде разместить: название учебного заведения, кафедры, учебной дисциплины, вид работы (реферат-презентация), название темы, реквизиты автора, место (г. Курск) и год. Размеры и цвета шрифта выбирать в соответствии с правилами визуализации.

2. Аналогичным образом создать макет второго слайда – плана реферата-презентации и разместить на нем путем копирования из структурированного текста необходимую информацию.

3. Соблюдая общие рекомендации, правила компоновки объектов на слайде и основные правила использования цвета (**Приложение В**) создать не менее десяти слайдов по теме презентации, копируя необходимый структурированный учебный материал из файла.

Вопросы для самоконтроля

1. На основе сочетания чьих и каких форм деятельности осуществляется обеспечение информационной безопасности?

2. На основе разграничения полномочий каких органов власти строится система обеспечения информационной безопасности?

3. Кто определяет состав системы обеспечения информационной безопасности?

4. Назовите органы власти, которые составляют организационную основу системы обеспечения информационной безопасности и принимают участие в решении задач по обеспечению информационной безопасности.

5. Назовите участников системы обеспечения информационной безопасности?

6. Раскройте сущность принципов, на которых основывается деятельность государственных органов по обеспечению информационной безопасности.

7. Перечислите задачи, решаемые государственными органами в рамках их деятельности по обеспечению информационной безопасности.

8. Перечислите задачи, решаемые государственными органами в рамках их деятельности по развитию и совершенствованию системы обеспечения.

9. Раскройте сущность термина «организационная защита информации».

10. Назовите организационно-распорядительные документы, связанные с защитой сведений конфиденциального характера.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

4. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

6. Указ Президента РФ от 31.12.2015 №683 «О стратегии национальной безопасности Российской Федерации».

7. Указ Президента РФ от 05.12.2016 №646 «О доктрине информационной безопасности Российской Федерации.

8. Указ Президента РФ от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».

9. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. – Старый Оскол : ТНТ, 2013. – 384 с.

10. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

2.6. Тема 6. Защита информации в компьютерных системах от случайных угроз и традиционного шпионажа

Структура (план)

1. Организация дублирования информации.
2. Повышение надежности и отказоустойчивости компьютерных систем.
3. Блокировка ошибочных операций и оптимизация взаимодействия пользователей с компьютерной системой.
4. Минимизация ущерба от аварий и стихийных бедствий.
5. Защита конфиденциальных информационных ресурсов, противодействие наблюдению в оптическом диапазоне и прослушиванию.
6. Методы и средства защиты от электромагнитных излучений и наводок

Глоссарий

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры.

Стратегическими целями обеспечения информационной безопасности в экономической сфере являются сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной

отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности.

Стратегической целью обеспечения информационной безопасности в области науки, технологий и образования является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности.

Стратегической целью обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

Критическая информационная инфраструктура – совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой.

Объекты критической информационной инфраструктуры – информационные системы и информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, в сфере здравоохранения, транспорта, связи, в кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг.

Организационная защита информации – составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Средства защиты сведений, составляющих государственные секреты – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственные секреты, средства, в которых они реализованы, а также средства контроля эффективности защиты государственных секретов.

Средства технической защиты информации – технические средства, предназначенные для защиты информации, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Практическое занятие №6

Тема: «Поиск и систематизация информации на тему «Защита информации в компьютерных системах от случайных угроз и традиционного шпионажа». Разработка текстового документа и его презентация»

Суть практического занятия: Оценка уровней сформированности компетенций в категориях УМЕТЬ, ВЛАДЕТЬ по результатам выполнения заданий с использованием возможностей компьютерных технологий для поиска информации на заданную тему и оформления рефератов-презентаций.

Самостоятельная работа

Кейс-задача. Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов:

1. Организация дублирования информации.

2. Повышение надежности и отказоустойчивости компьютерных систем.

3. Блокировка ошибочных операций и оптимизация взаимодействия пользователей с компьютерной системой.

4. Минимизация ущерба от аварий и стихийных бедствий.

5. Защита конфиденциальных информационных ресурсов, противодействие наблюдению в оптическом диапазоне и прослушиванию.

6. Методы и средства защиты от электромагнитных излучений и наводок.

Методика выполнения:

Алгоритм структурирования учебного материала.

1. Включить персональный компьютер, войти в работу с СПС КонсультантПлюс (Гарант) или сеть Интернета, найти в базе данных соответствующую теме информацию в текстах современных НПА, скопировать её на отдельный файл в текстовом редакторе WORD и оформить в виде Тезауруса в соответствии с требованиями к оформлению текстовых документов.

2. Выполнить структурно-логический анализ отобранного учебного материала: выделить по тексту (цветом, фоном) главное содержание (ядро), основные положения, понятия и определения по теме реферата-презентации.

3. Построить структурно-логическую схему учебной информации (план презентации).

4. Расположить учебный материал с учетом логики формирования учебных понятий, лишний текст удалить.

5. Выполнить подбор опорных сигналов (ключевых слов, символов, фрагментов схем) и их кодировку (при необходимости).

6. Выполнить компоновку учебного материала в блоки (содержание слайдов) и составить первичный вариант (макет) презентации.

7. Критически осмыслить первичный вариант, при необходимости перекомпоновать, перестроить, упростить отобранный учебный материал.

Алгоритм создания реферата-презентации.

Приветствуются любые другие алгоритмы создания

презентаций в пределах возможностей графического редактора Power Point и других офисных программ.

1. На титульном слайде разместить: название учебного заведения, кафедры, учебной дисциплины, вид работы (реферат-презентация), название темы, реквизиты автора, место (г. Курск) и год. Размеры и цвета шрифта выбирать в соответствии с правилами визуализации.

2. Аналогичным образом создать макет второго слайда – плана реферата-презентации и разместить на нем путем копирования из структурированного текста необходимую информацию.

3. Соблюдая общие рекомендации, правила компоновки объектов на слайде и основные правила использования цвета (**Приложение В**) создать не менее десяти слайдов по теме презентации, копируя необходимый структурированный учебный материал из файла.

Вопросы для самоконтроля

1. Охарактеризуйте основные виды случайных угроз и традиционного шпионажа в компьютерных системах.

2. Раскройте сущность формальных и неформальных методов и средств защиты информации в компьютерных системах.

3. Раскройте сущность технических методов и средств защиты информации в компьютерных системах.

4. Раскройте сущность программных методов и средств защиты информации в компьютерных системах.

5. Организация дублирования информации в компьютерных системах.

6. Раскройте методы и способы повышения надежности и отказоустойчивости компьютерных систем.

7. Блокировка ошибочных операций и оптимизация взаимодействия пользователей с компьютерной системой.

8. Минимизация ущерба от аварий и стихийных бедствий в компьютерных системах.

9. Защита конфиденциальных информационных ресурсов, противодействие наблюдению в оптическом диапазоне и прослушиванию.

10. Раскройте сущность методов и средств защиты от электромагнитных излучений и наводок в компьютерных системах.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3. Указ Президента РФ от 05.12.2016 №646 «О доктрине информационной безопасности Российской Федерации.

4. Указ Президента РФ от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».

5. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. – Старый Оскол : ТНТ, 2013. – 384 с.

6. Калуцкий, И.В. Программно-аппаратные средства защиты информационных систем [Текст] : учебное пособие / И.В. Калуцкий, А.Г. Спеваков ; Юго-Зап. гос. ун-т. – Курск : ЮЗГУ, 2014. – 179 с.

7. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Елена Анатольевна Богданова [и др.]. – М. : Национальный Открытый Университет "ИНТУИТ", 2013. – 743 с.

8. Технические средства и методы защиты информации [Текст] : учебное пособие / Роман Валерьевич Мещеряков [и др.] ; под ред. А. П. Зайцева и А. А. Шелупанова. – М. : Горячая линия-Телеком, 2012. – 616 с.

9. Ищейнов, В. Я.Защита конфиденциальной информации [Текст] : учебное пособие / Вячеслав Яковлевич Ищейнов, Михаил Владимирович Мецатунян. – М. : Форум, 2013. – 256 с.

10. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

2.7. Тема 7. Методы и средства защиты информации от несанкционированного доступа и изменения структур в компьютерных системах

Структура (план)

1. Защита информации в компьютерных системах от несанкционированного доступа.
2. Методы и средства защиты от несанкционированного изменения структур компьютерных систем.
3. Криптографические методы защиты информации.
4. Криптология, криптография и криптоанализ.
5. Классификация криптографических методов.
6. Симметричное и асимметричное шифрование.
7. Электронная подпись.

Глоссарий

Корпоративная информационная система – информационная система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Модификация информации (modification of information) – обнаруженное или необнаруженное несанкционированное или случайное изменение информации.

Мошенничество в сфере компьютерной информации – хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных

средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Неправомерное использование информационных ресурсов – использование информационных ресурсов без соответствующих прав или с нарушением установленных правил, законодательства государств, сторон либо норм международного права.

Носители сведений, составляющих государственную тайну – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Носители секретной информации – материальные объекты, в том числе физические поля, в которых секретная информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Объект защиты информации – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Оценка соответствия требованиям по защите информации – прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Право на доступ к информации – право каждого гражданина свободно осуществлять поиск информации и получать ее от государственных органов и организаций, иных органов и организаций, наделенных государством властными полномочиями, органов местного самоуправления (далее - органов и организаций), их должностных лиц, обладающих этой информацией на законных основаниях.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Аутентификация (англ. authentication) – 1) удостоверение подлинности документа, подписи, личности человека; 2) подтверждение принадлежности платежной карточки ее держателю, проводимое путем установления личности держателя карточки и соответствия реквизитов, нанесенных на карточку. Возможное написание термина – аутентикация.

Аутентификация электронного документа – процедура подтверждения подлинности электронного документа путем проверки цифровой подписи электронного документа по ключу проверки подписи отправителя и проверки контрольной суммы файла на соответствие сумме, заявленной автором этого файла.

Аутентичность (authenticity) – свойство, гарантирующее, что субъект или ресурс идентичны заявленным. Аутентичность применяется к таким субъектам, как пользователи, к процессам, системам и информации.

Единая система идентификации и аутентификации – федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах.

Криптографическая аутентификация (cryptographic authentication) – аутентификация, основанная на цифровой подписи, коде аутентификации сообщения, генерируемых в соответствии с криптографическим ключом.

Техника защиты информации – средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Практическое занятие №7

Тема: «Поиск и систематизация информации на тему «Методы и средства защиты информации от несанкционированного доступа и изменения структур в компьютерных системах». Разработка текстового документа и его презентация»

Суть практического занятия: Оценка уровней сформированности компетенций в категориях УМЕТЬ, ВЛАДЕТЬ по результатам выполнения заданий с использованием возможностей компьютерных технологий для поиска информации на заданную тему и оформления рефератов-презентаций.

Самостоятельная работа

Кейс-задача №1. Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов:

1. Защита информации в компьютерных системах от несанкционированного доступа.
2. Методы и средства защиты от несанкционированного изменения структур компьютерных систем.
3. Криптографические методы защиты информации.

4. Криптология, криптография и криптоанализ.
5. Классификация криптографических методов.
6. Симметричное и асимметричное шифрование.
7. Электронная подпись.

Методика выполнения:

Алгоритм структурирования учебного материала.

1. Включить персональный компьютер, войти в работу с СПС КонсультантПлюс (Гарант) или сеть Интернета, найти в базе данных соответствующую теме информацию в текстах современных НПА, скопировать её на отдельный файл в текстовом редакторе WORD и оформить в виде Тезауруса в соответствии с требованиями к оформлению текстовых документов.

2. Выполнить структурно-логический анализ отобранного учебного материала: выделить по тексту (цветом, фоном) главное содержание (ядро), основные положения, понятия и определения по теме реферата-презентации.

3. Построить структурно-логическую схему учебной информации (план презентации).

4. Расположить учебный материал с учетом логики формирования учебных понятий, лишний текст удалить.

5. Выполнить подбор опорных сигналов (ключевых слов, символов, фрагментов схем) и их кодировку (при необходимости).

6. Выполнить компоновку учебного материала в блоки (содержание слайдов) и составить первичный вариант (макет) презентации.

7. Критически осмыслить первичный вариант, при необходимости перекомпоновать, перестроить, упростить отобранный учебный материал.

Алгоритм создания реферата-презентации.

Приветствуются любые другие алгоритмы создания презентаций в пределах возможностей графического редактора Power Point и других офисных программ.

1. На титульном слайде разместить: название учебного заведения, кафедры, учебной дисциплины, вид работы (реферат-презентация), название темы, реквизиты автора, место (г. Курск) и год. Размеры и цвета шрифта выбирать в соответствии с правилами визуализации.

2. Аналогичным образом создать макет второго слайда – плана реферата-презентации и разместить на нем путем копирования из структурированного текста необходимую информацию.

3. Соблюдая общие рекомендации, правила компоновки объектов на слайде и основные правила использования цвета (**Приложение В**) создать не менее десяти слайдов по теме презентации, копируя необходимый структурированный учебный материал из файла.

Вопросы для самоконтроля

1. Раскройте сущность защиты информации в компьютерных системах от несанкционированного доступа.
2. Методы и средства защиты от несанкционированного изменения структур компьютерных систем.
3. Раскройте классификацию криптографических методов защиты информации в компьютерных системах.
4. Раскройте понятия криптология, криптография и криптоанализ, симметричное и асимметричное шифрование.
5. Что такое электронная подпись и её роль в защите информации в компьютерных системах.
6. Раскройте методы и средства обеспечения целостности информации в компьютерных системах.
7. Назовите способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации в компьютерных системах.
8. Назовите способы разграничение доступа к элементам защищаемой информации в компьютерных системах.
9. Криптографическое закрытие защищаемой информации, хранимой на носителях.
10. Криптографическое закрытие защищаемой информации в процессе непосредственной ее обработки.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
3. Указ Президента РФ от 05.12.2016 №646 «О доктрине информационной безопасности Российской Федерации.

4. Указ Президента РФ от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».

5. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. – Старый Оскол : ТНТ, 2013. – 384 с.

6. Калуцкий, И.В. Программно-аппаратные средства защиты информационных систем [Текст] : учебное пособие / И.В. Калуцкий, А.Г. Спеваков ; Юго-Зап. гос. ун-т. – Курск : ЮЗГУ, 2014. – 179 с.

7. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Елена Анатольевна Богданова [и др.]. – М. : Национальный Открытый Университет "ИНТУИТ", 2013. – 743 с.

8. Технические средства и методы защиты информации [Текст] : учебное пособие / Роман Валерьевич Мещеряков [и др.] ; под ред. А. П. Зайцева и А. А. Шелупанова. – М. : Горячая линия-Телеком, 2012. – 616 с.

9. Ищейнов, В. Я.Защита конфиденциальной информации [Текст] : учебное пособие / Вячеслав Яковлевич Ищейнов, Михаил Владимирович Мецатунян. – М. : Форум, 2013. – 256 с.

10. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

2.8. Тема 8. Защита информации в распределенных компьютерных системах

Структура (план)

1. Особенности защиты информации в распределенных компьютерных системах.
2. Характеристика угроз информационной безопасности в распределенных компьютерных системах.
3. Защита информации в каналах связи.
4. Межсетевое экранирование.
5. Подтверждение подлинности информации и взаимодействующих процессов.
6. Практические рекомендации пользователям глобальной сети Интернет по обеспечению информационной безопасности.

Глоссарий

Распределенная компьютерная система – это множество сосредоточенных компьютерных систем, связанных в единую систему с помощью коммуникационной подсистемы.

Распределенные компьютерные системы строятся по сетевым технологиям и представляют собой вычислительные сети.

Коммутационная подсистема распределенной компьютерной системы включает:

- *коммутационные модули* – которые обеспечивают передачу полученного пакета другому коммутационному модулю или абонентскому пункту в соответствии с маршрутом передачи. Коммутационный модуль называют также центром коммутации пакетов);
- *каналы связи* – которые объединяют элементы сети в единую сеть и могут иметь различную скорость передачи данных;
- *концентраторы* – которые используются для уплотнения информации перед передачей ее по высокоскоростным каналам;
- *межсетевые шлюзы* (мосты) – которые используются для связи сети с ЛВС или для связи сегментов глобальных сетей. С помощью мостов связываются сегменты сети с одинаковыми сетевыми протоколами.

С точки зрения защиты информации в распределенных компьютерных системах разделяют вычислительные сети на *корпоративные* и *общедоступные*.

В корпоративных сетях все элементы принадлежат одному ведомству, за исключением, может быть, каналов связи. В таких системах имеется возможность проводить единую политику обеспечения безопасности информации по всей сети.

В общедоступных коммерческих сетях во главу угла ставится распространение информации, а вопросы защиты собственных информационных ресурсов решаются, в основном, на уровне пользователей.

Меры против искажения и потери информации в каналах связи – в распределенных компьютерных системах должны быть предусмотрены дублирующие маршруты доставки сообщений, такие сложные системы должны строиться как адаптивные, в которых обеспечивается постоянный контроль работоспособности элементов системы и возможность продолжения функционирования даже в условиях отказов отдельных подсистем.

Искажения информации в каналах связи фиксируются и частично исправляются с помощью помехоустойчивого кодирования. Потери информации исключаются за счет использования контроля и учета принятых сообщений, а также за счет применения протоколов обмена с подтверждением о приеме информации.

В распределенных компьютерных системах все потенциальные преднамеренные угрозы безопасности информации делят на две группы: *пассивные* и *активные*.

К *пассивным* относятся угрозы, целью реализации которых является получение информации о системе путем прослушивания каналов связи (злоумышленник может получить информацию путем перехвата незашифрованных сообщений или путем анализа трафика (потока сообщений), накапливая информацию об интенсивности обмена отдельных абонентов, о структуре сообщений, о маршрутах доставки сообщений и т.п.).

Активные угрозы предусматривают воздействие на передаваемые сообщения в сети и несанкционированную передачу фальсифицированных сообщений с целью воздействия на информационные ресурсы объектов распределенных компьютерных систем и дестабилизацию функционирования системы. Возможно также непосредственное воздействие на коммуникационную подсистему с целью повреждения аппаратных средств передачи информации.

Передаваемые в распределенных компьютерных системах сообщения могут *несанкционированно модифицироваться или уничтожаться.* Злоумышленник может размножать перехваченные сообщения, нарушать их очередность следования, изменять маршрут доставки, подменять сообщения, может предпринимать попытки несанкционированного доступа к информационным ресурсам удаленного объекта компьютерной системы, осуществления несанкционированного изменения программной структуры компьютерной системы путем внедрения вредительских программ.

Все методы и средства, обеспечивающие безопасность информации в защищенной вычислительной сети, могут быть распределены по группам:

- обеспечение безопасности информации в пользовательской подсистеме и специализированных коммуникационных КС;
- защита информации на уровне подсистемы управления сетью;
- защита информации в каналах связи;
- обеспечение контроля подлинности взаимодействующих процессов.

Особенностью защиты объектов распределённой компьютерной системы является необходимость поддержки механизмов аутентификации и разграничения доступа удаленных процессов к ресурсам объекта, а также наличие в сети специальных коммуникационных компьютерных систем.

Для защиты информации, передаваемой по каналам связи, применяется комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации. Наиболее надежным и универсальным методом защиты информации в каналах связи является шифрование.

Шифрование на абонентском уровне позволяет защитить рабочую информацию от утраты конфиденциальности и навязывания ложной информации.

Линейное шифрование позволяет, кроме того, защитить служебную информацию. Не имея доступа к служебной информации, злоумышленник не может фиксировать факт передачи между конкретными абонентами сети, изменить адресную часть сообщения с целью его переадресации.

Противодействие ложным соединениям абонентов (процессов) обеспечивается применением целого ряда процедур взаимного подтверждения подлинности абонентов или процессов. Против удаления, явного искажения, переупорядочивания, передачи дублей сообщений используется механизм квитирования, нумерации сообщений или использования информации о времени отправки сообщения. Эти служебные данные должны быть зашифрованы.

Для блокирования угроз физического воздействия на каналы связи (нарушение линий связи или постановка помех в радиоканалах) необходимо иметь дублирующие каналы с возможностью автоматического перехода на их использование.

Практическое занятие №8

Тема: «Поиск и систематизация информации на тему «Защита информации в распределенных компьютерных системах». Разработка текстового документа и его презентация»

Суть практического занятия: Оценка уровней сформированности компетенций в категориях УМЕТЬ, ВЛАДЕТЬ по результатам выполнения заданий с использованием возможностей компьютерных технологий для поиска информации на заданную тему и оформления рефератов-презентаций.

Самостоятельная работа

Кейс-задача. Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов:

1. Особенности защиты информации в распределенных компьютерных системах.
2. Характеристика угроз информационной безопасности в распределенных компьютерных системах.
3. Защита информации в каналах связи.
4. Межсетевое экранирование.
5. Подтверждение подлинности информации и взаимодействующих процессов.
6. Практические рекомендации пользователям глобальной сети Интернет по обеспечению информационной безопасности.

Методика выполнения:

Алгоритм структурирования учебного материала.

1. Включить персональный компьютер, войти в работу с СПС КонсультантПлюс (Гарант) или сеть Интернета, найти в базе данных соответствующую теме информацию в текстах современных НПА, скопировать её на отдельный файл в текстовом редакторе WORD и оформить в виде Тезауруса в соответствии с требованиями к оформлению текстовых документов.

2. Выполнить структурно-логический анализ отобранного учебного материала: выделить по тексту (цветом, фоном) главное содержание (ядро), основные положения, понятия и определения по теме реферата-презентации.

3. Построить структурно-логическую схему учебной информации (план презентации).

4. Расположить учебный материал с учетом логики формирования учебных понятий, лишний текст удалить.

5. Выполнить подбор опорных сигналов (ключевых слов, символов, фрагментов схем) и их кодировку (при необходимости).

6. Выполнить компоновку учебного материала в блоки (содержание слайдов) и составить первичный вариант (макет) презентации.

7. Критически осмыслить первичный вариант, при необходимости перекомпоновать, перестроить, упростить отобранный учебный материал.

Алгоритм создания реферата-презентации.

Приветствуются любые другие алгоритмы создания презентаций в пределах возможностей графического редактора Power Point и других офисных программ.

1. На титульном слайде разместить: название учебного заведения, кафедры, учебной дисциплины, вид работы (реферат-презентация), название темы, реквизиты автора, место (г. Курск) и год. Размеры и цвета шрифта выбирать в соответствии с правилами визуализации.

2. Аналогичным образом создать макет второго слайда – плана реферата-презентации и разместить на нем путем копирования из структурированного текста необходимую информацию.

3. Соблюдая общие рекомендации, правила компоновки

объектов на слайде и основные правила использования цвета (**Приложение В**) создать не менее десяти слайдов по теме презентации, копируя необходимый структурированный учебный материал из файла.

Вопросы для самоконтроля

1. Дайте характеристику распределенной компьютерной системы и особенностей её построения.
2. Раскройте состав и назначение элементов коммутационной подсистема распределенной компьютерной системы.
3. Раскройте особенности защиты информации в корпоративных и общедоступных вычислительные сетях.
4. Дайте характеристику угроз информационной безопасности в распределенных компьютерных системах.
5. Раскройте меры против искажения и потери информации в каналах связи.
6. Раскройте сущность пассивных и активных потенциальных преднамеренных угроз безопасности информации в распределенных компьютерных системах.
7. Раскройте сущность несанкционированного модифицирования или уничтожения передаваемые в распределенных компьютерных системах сообщений.
8. Что такое межсетевое экранирование, шифрование на абонентском уровне и линейное шифрование как методы подтверждения подлинности информации и взаимодействующих процессов.
9. Раскройте особенности защиты объектов распределённой компьютерной системы.
10. Как обеспечивается противодействие ложным соединениям абонентов (процессов) в распределенных компьютерных системах.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
3. Указ Президента РФ от 05.12.2016 №646 «О доктрине информационной безопасности Российской Федерации.

4. Указ Президента РФ от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».

5. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. – Старый Оскол : ТНТ, 2013. – 384 с.

6. Калуцкий, И.В. Программно-аппаратные средства защиты информационных систем [Текст] : учебное пособие / И.В. Калуцкий, А.Г. Спеваков ; Юго-Зап. гос. ун-т. – Курск : ЮЗГУ, 2014. – 179 с.

7. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Елена Анатольевна Богданова [и др.]. – М. : Национальный Открытый Университет "ИНТУИТ", 2013. – 743 с.

8. Технические средства и методы защиты информации [Текст] : учебное пособие / Роман Валерьевич Мещеряков [и др.] ; под ред. А. П. Зайцева и А. А. Шелупанова. – М. : Горячая линия-Телеком, 2012. – 616 с.

9. Ищейнов, В. Я.Защита конфиденциальной информации [Текст] : учебное пособие / Вячеслав Яковлевич Ищейнов, Михаил Владимирович Мецатунян. – М. : Форум, 2013. – 256 с.

10. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

2.9. Тема 9. Защита компьютерных систем от вирусов и вредоносных программ

Структура (план)

1. Классификация компьютерных вирусов и вредоносных программ.
2. Файловые, загрузочные и сетевые вирусы.
3. Методы и средства борьбы с вирусами и вредоносными программами.
4. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения

Глоссарий

Компьютерный вирус – это программа, нарушающая нормальную работу других программ и компьютерной техники. Она обладает способностью самовоспроизведения, распространения, внедрения в другие программы.

Компьютерный вирус — это специально написанная, небольшая по размерам программа (т. е. некоторая совокупность выполняемого кода), которая может «приписывать» себя к другим программам («заражать» их), создавать свои копии и внедрять их в файлы, системные области компьютера и т. д., а также выполнять различные нежелательные действия на компьютере.

Своим названием компьютерные вирусы обязаны определенному сходству с биологическими вирусами по: способности к саморазмножению; высокой скорости распространения;избирательности поражаемых систем (каждый вирус поражает только определенные системы или однородные группы систем); способности «заражать» еще незараженные системы.

Условно можно *классифицировать вирусы по следующим признакам*: по среде обитания вируса; по способу заражения среды обитания; по деструктивным возможностям; по особенностям алгоритма вируса.

Загру́зочный ви́рус – компьютерный вирус, записывающийся в первый сектор гибкого или жёсткого диска и выполняющийся при загрузке компьютера с идущих после главной загрузочной записи (MBR), но до первого загрузочного сектора раздела.

Файловый вирус – компьютерный вирус, который для своего размножения использует файловую систему, внедряясь в исполняемые файлы практически любой операционной системы.

Сетевые вирусы – это особые программы, которые распространяются через интернет. Для этого они используют сетевые протоколы, общие для всех пользователей во всем мире.

Для защиты от вирусов можно использовать:

• *общие средства защиты информации*, которые полезны также как и страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;

• *профилактические меры*, позволяющие уменьшить вероятность заражения вирусом;

• *специализированные программы* для защиты от вирусов.

Общие средства защиты – имеются две основные разновидности, обеспечивающие: 1) копирование информации – создание копий файлов и системных областей дисков; 2) разграничение доступа, которое предотвращает несанкционированное использование информации, в частности защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными. Различают следующие виды антивирусных программ:

- программы-фаги (сканеры);
- программы-ревизоры (CRC-сканеры);
- программы-блокировщики;
- программы-иммунизаторы.

Программы-фаги (сканеры) – используют для обнаружения вирусов метод сравнения с эталоном, метод эвристического анализа и некоторые другие методы. Программы-фаги осуществляют поиск характерной для конкретного вируса маски путем сканирования в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Программы-фаги не только находят зараженные вирусами файлы, но и «лечат» их, т. е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В

начале работы программы-фаги сканируют оперативную память, обнаруживают вирусы и уничтожают их и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги — программы-фаги, предназначенные для поиска и уничтожения большого числа вирусов.

Программы-ревизоры (CRC-сканеры) – используют для поиска вирусов метод обнаружения изменений. Принцип работы CRC-сканеров основан на подсчете CRC-сумм (кодов циклического контроля) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы, а также некоторая другая информация (длины файлов, даты их последней модификации и др.) затем сохраняются в БД антивируса. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в БД, с реально подсчитанными значениями. Если информация о файле, записанная в БД, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. Как правило, сравнение состояний производят сразу после загрузки ОС.

Программы-блокировщики – реализуют метод антивирусного мониторинга. Антивирусные блокировщики – это резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие об этом пользователю. К «вирусо-опасным» ситуациям относятся вызовы, которые характерны для вирусов в моменты их размножения (вызовы на открытие для записи в выполняемые файлы, запись в загрузочные секторы дисков или MBR винчестера, попытки программ остаться резидентно и т. п.).

Программы-иммунизаторы – это программы, предотвращающие заражение файлов. Иммунизаторы делятся на два типа: 1) иммунизаторы, сообщающие о заражении, 2) иммунизаторы, блокирующие заражение каким-либо типом вируса.

Иммунизаторы, сообщающие о заражении – обычно записываются в конец файлов и при запуске файла каждый раз проверяют его на изменение. У таких иммунизаторов имеется один серьезный недостаток – они не могут обнаружить заражение стелс-вирусом. Поэтому этот тип иммунизаторов практически не используются в настоящее время.

Иммунизаторы, блокирующие заражение – защищают систему от поражения вирусом определенного вида. Они модифицируют

программу или диск таким образом, чтобы это не отражалось на их работе, вирус при этом воспринимает их зараженными и поэтому не внедряется. Такой тип иммунизации не может быть универсальным, поскольку нельзя иммунизировать файлы от всех известных вирусов. Однако в качестве полумеры подобные иммунизаторы могут вполне надежно защитить компьютер от нового неизвестного вируса вплоть до того момента, когда он будет определяться антивирусными сканерами.

Практическое занятие №9

Тема: «Поиск и систематизация информации на тему «Защита компьютерных систем от вирусов и вредоносных программ». Разработка текстового документа и его презентация»

Суть практического занятия: Оценка уровней сформированности компетенций в категориях УМЕТЬ, ВЛАДЕТЬ по результатам выполнения заданий с использованием возможностей компьютерных технологий для поиска информации на заданную тему и оформления рефератов-презентаций.

Самостоятельная работа

Кейс-задача №1. Разработать реферат-презентацию на заданную тему с использованием содержания требований найденных в СПС и Интернете сосовременных нормативных правовых актов и программ системы Microsoft Office в объеме следующих вопросов:

1. Классификация компьютерных вирусов и вредоносных программ.
2. Файловые, загрузочные и сетевые вирусы.
3. Методы и средства борьбы с вирусами и вредоносными программами.
4. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения

Методика выполнения:

Алгоритм структурирования учебного материала.

1. Включить персональный компьютер, войти в работу с СПС КонсультантПлюс (Гарант) или сеть Интернета, найти в базе данных соответствующую теме информацию в текстах современных НПА,

скопировать её на отдельный файл в текстовом редакторе WORD и оформить в виде Тезауруса в соответствии с требованиями к оформлению текстовых документов.

2. Выполнить структурно-логический анализ отобранного учебного материала: выделить по тексту (цветом, фоном) главное содержание (ядро), основные положения, понятия и определения по теме реферата-презентации.

3. Построить структурно-логическую схему учебной информации (план презентации).

4. Расположить учебный материал с учетом логики формирования учебных понятий, лишний текст удалить.

5. Выполнить подбор опорных сигналов (ключевых слов, символов, фрагментов схем) и их кодировку (при необходимости).

6. Выполнить компоновку учебного материала в блоки (содержание слайдов) и составить первичный вариант (макет) презентации.

7. Критически осмыслить первичный вариант, при необходимости перекомпоновать, перестроить, упростить отобранный учебный материал.

Алгоритм создания реферата-презентации.

Приветствуются любые другие алгоритмы создания презентаций в пределах возможностей графического редактора Power Point и других офисных программ.

1. На титульном слайде разместить: название учебного заведения, кафедры, учебной дисциплины, вид работы (реферат-презентация), название темы, реквизиты автора, место (г. Курск) и год. Размеры и цвета шрифта выбирать в соответствии с правилами визуализации.

2. Аналогичным образом создать макет второго слайда – плана реферата-презентации и разместить на нем путем копирования из структурированного текста необходимую информацию.

3. Соблюдая общие рекомендации, правила компоновки объектов на слайде и основные правила использования цвета (**Приложение В**) создать не менее десяти слайдов по теме презентации, копируя необходимый структурированный учебный материал из файла.

Вопросы для самоконтроля

1. Что такое копьютерные вирусы и по каким признакам их условно можно классифицировать?

2. Дайте определение и покажите отличия загрузочного, файлового и сетевого вирусов.

3. Какие средства, меры и программы можно использовать для защиты от вирусов.

4. Раскройте разновидности общих средств защиты от вредоносных программ.

5. Раскройте виды специальных программ для обнаружения, удаления и защиты от компьютерных вирусов.

6. Охарактеризуйте антивирусные программы-фаги (сканеры).

7. Охарактеризуйте антивирусные программы-ревизоры (CRC-сканеры).

8. Охарактеризуйте антивирусные программы-блокировщики.

9. Охарактеризуйте антивирусные программы-иммунизаторы, сообщающие о заражении.

10. Охарактеризуйте антивирусные программы-иммунизаторы, блокирующие заражение.

Литература

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3. Указ Президента РФ от 05.12.2016 №646 «О доктрине информационной безопасности Российской Федерации.

4. Указ Президента РФ от 09.05.2017 №203 «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».

5. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. – Старый Оскол : ТНТ, 2013. – 384 с.

6. Калуцкий, И.В. Программно-аппаратные средства защиты информационных систем [Текст] : учебное пособие / И.В. Калуцкий, А.Г. Спеваков ; Юго-Зап. гос. ун-т. – Курск : ЮЗГУ, 2014. – 179 с.

7. Богомолова, О Б.Защита компьютера от вредоносных воздействий [Электронный ресурс]: практикум / О Б. Богомолова, Д.Ю.

Усенков. – М.: БИНОМ. Лаборатория знаний, 2012. – 179с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=221695&sr=1

8. Технические средства и методы защиты информации [Текст] : учебное пособие / Роман Валерьевич Мещеряков [и др.] ; под ред. А. П. Зайцева и А. А. Шелупанова. – М. : Горячая линия-Телеком, 2012. – 616 с.

9. Ищейнов, В. Я.Защита конфиденциальной информации [Текст] : учебное пособие / Вячеслав Яковлевич Ищейнов, Михаил Владимирович Мецатунян. – М. : Форум, 2013. – 256 с.

10. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

3. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

3.1. Основная и дополнительная литература

Основная

1. Информационная безопасность и защита информации [Текст] : учебное пособие / Ю. Ю. Громов [и др.]. – Старый Оскол : ТНТ, 2013. – 384 с.

2. Калуцкий, И.В. Программно-аппаратные средства защиты информационных систем [Текст] : учебное пособие / И.В. Калуцкий, А.Г. Спеваков ; Юго-Зап. гос. ун-т. – Курск : ЮЗГУ, 2014. – 179 с.

3. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Елена Анатольевна Богданова [и др.]. – М. : Национальный Открытый Университет "ИНТУИТ", 2013. – 743 с.

4. Технические средства и методы защиты информации [Текст] : учебное пособие / Роман Валерьевич Мещеряков [и др.] ; под ред. А. П. Зайцева и А. А. Шелупанова. – М. : Горячая линия-Телеком, 2012. – 616 с.

Дополнительная

5. Богомолова, О Б.Защита компьютера от вредоносных воздействий [Электронный ресурс]: практикум / О Б. Богомолова, Д.Ю. Усенков. – М.: БИНОМ. Лаборатория знаний, 2012. – 179с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=221695&sr=1

6. Защита данных геоинформационных систем [Текст] / Людмила Климентьевна Бабенко [и др.]. – М. : Гелиос АРВ, 2010. - 336 с. : ил.

7. Ищейнов, В. Я.Защита конфиденциальной информации [Текст] : учебное пособие / Вячеслав Яковлевич Ищейнов, Михаил Владимирович Мецатунян. – М. : Форум, 2013. – 256 с.

8. Носенко, В. А. Защита интеллектуальной собственности [Текст] : учебное пособие / Владимир Андреевич Носенко, Анна Вадимовна Степанова. – Старый Оскол : ТНТ, 2013. – 192 с.

9. Перетолчин, А.С. Защита Windows от сбоев [Электронный

ресурс]: практикум / А.С. Перетолчин. – Новосибирск: Сибирское университетское издательство, 2008. – 112 с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=57378&sr=1

10. Сергеева, Ю.С. Защита информации. Конспект лекций [Электронный ресурс]: учебное пособие / Ю.С. Сергеева. – М.: А-Приор, 2011. – 128 с. // Универ. библ. online – http://biblioclub.ru/index.php?page=book&id=72670&sr=1

11. Сычев, Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебно-практическое пособие / Ю.Н. Сычёв. – М.: Евразийский открытый институт, 2010. – 328 с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=90790&sr=1

12. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]: курс лекций. – М.: Интернет-Университет Информационных Технологий, 2011. – 138 с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=233763&sr=1

3.2. Перечень методических указаний

1. Организационно-правовые механизмы обеспечения информационной безопасности [Электронный ресурс]: методические указания по подготовке к практическим занятиям для студентов всех форм обучения специальности 030900.68 «Юриспруденция» / Юго-Западный государственный университет ; сост. А. А. Гребеньков [и др.]. – Электрон. текстовые дан. (534 КБ). - Курск : ЮЗГУ, 2014. - 30 с. : прил.

2. ГОСТ Р ИСО/МЭК 15408-2-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий [Текст] . Ч. 2 : Функциональные требования безопасности. – Введ. 2009.10.01 ; взамен ГОСТ Р ИСО/МЭК 15408-2-2002. – М. : Стандартинформ, 2009. – 167 с. – (Национальный стандарт РФ).

3. ГОСТ Р ИСО/МЭК 15408-3-2008. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Информационная технология [Текст] . Ч. 3 : Требования доверия к безопасности. – Введ. 2009.10.01 ; взамен ГОСТ Р ИСО/МЭК 15408-3-2002. – М. : Стандартинформ,

2009. – 112 с. – (Национальный стандарт РФ).

4. Стохастические методы и средства защиты информации в компьютерных системах и сетях [Текст] / М. А. Иванов [и др.] ; под ред. И. Ю. Жукова. – М. : КУДИЦ-ПРЕСС, 2009. – 512 с. - ISBN 978-5-91136-068-9 : 811р. 36к. Кол-во экземпляров: всего – 1

5. Дидактические материалы: раздаточный материал (задания к практическим занятиям, бланки отчетов), электронные версии раздаточного материала.

3.3. Используемые информационные технологии и перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Мультимедийные технологии визуализации учебной информации.
2. Сетевая версия СПС КонсультантПлюс, СПС Гарант,
3. Пакет программ Microsoft Office, и др.
4. Сервер государственных органов России [Электронный ресурс]. http://www.gov.ru/
5. Президент Российской Федерации. Официальный сайт. [Электронный ресурс]. http://kremlin.ru/. http://www.gov.ru/main/page3.html
6. Правительство России. Официальный сайт. [Электронный ресурс]. http://www.government.ru/
7. Государственная Дума Федерального Собрания Российской Федерации. Официальный сайт. [Электронный ресурс]. http://www.duma.ru/
8. Совет Федерации Федерального Собрания Российской Федерации. Официальный сайт. [Электронный ресурс]. http://www.council.gov.ru/
9. Конституционный Суд РФ. Официальный сайт. [Электронный ресурс]. http://ks.rfnet.ru/
10. Верховный Суд РФ. Официальный сайт. [Электронный ресурс]. http://www.supcourt.ru/
11. Федеральные Арбитражные Суды РФ. [Электронный ресурс] http://www.arbitr.ru/

12. Официальный интернет-портал правовой информации. Государственная система правовой информации. [Электронный ресурс] http://pravo.fso.gov.ru/

13. http://crimestat.ru/ Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации. [Электронный ресурс].

14. 7. http://www.znanium.com/bookread.php?book=405000 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.

15. http://www.znanium.com/bookread.php?book=335362 Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное пособие / В. Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - Режим доступа:

16. http://www.knigafund.ru/books/172320 Правовое обеспечение национальных интересов Российской Федерации в информационной сфере. [Электронный ресурс]: Автор: Куняев Н.Н. Издательство: Логос, 2010 г. 346 с.

.

ПРИЛОЖЕНИЯ

Приложение А. Вопросы и задания для подготовки к зачету

№	Содержание вопросов	Баллы
1	Информационная безопасность и ее составные части	4
2	Понятия целостности, конфиденциальности, аутентичности и доступности информации	4
3	Защищенность информационных ресурсов, систем и технологий	4
4	Актуальность и важность проблемы обеспечения ИБ	4
5	Предпосылки, направления и перспективы киберпреступности	4
6	Основные понятия в области информационной безопасности	4
7	Объект, предмет и цели защиты информации	4
8	Аспекты ИБ: доступность, целостность, конфиденциальность	4
9.	Понятие угрозы ИБ. Классификация и характеристика угроз ИБ	4
10	Характеристики информационного ресурса как объекта защиты	4
11	Случайные и преднамеренные угрозы информационной безопасности	4
12	Внешние и внутренние угрозы информационной безопасности	4
13	Угрозы информационной безопасности стихийного и искусственного характера	4
14	Проявления, последствия и основные способы реализации угроз	4
15	Понятие правового обеспечения ИБ	4
16	Особенности информации как объекта права	4
17	Государственная политика РФ в области правового обеспечения	4
18	Уровни правового регулирования в сфере ИБ	4
19	Основные конституционные и правовые нормы в области информационной безопасности	4
20	Понятия банковской, коммерческой и служебной тайны	4
21	Наказания за преступления в сфере компьютерной информации	4
22	Зарубежное законодательство в области ИБ	4
23	Понятие организационного обеспечения ИБ	4
24	Характеристика организационных методов обеспечения ИБ	4
25	Структура государственных органов РФ, осуществляющих правотворчество и правоприменение в области ИБ	4
26	Организационно - распорядительные документы, связанные с защитой сведений конфиденциального характера	4
27	Концепция построения комплексной системы обеспечения ИБ и защиты информации	4
28	Организация дублирования информации	4

29	Повышение надежности и отказоустойчивости компьютерных систем	4
30	Блокировка ошибочных операций и оптимизация взаимодействия пользователей с компьютерной системой	4
31	Минимизация ущерба от аварий и стихийных бедствий	4
32	Защита конфиденциальных информационных ресурсов, противодействие наблюдению в оптическом диапазоне и прослушиванию	4
33	Методы и средства защиты от электромагнитных излучений и наводок	4
34	Защита информации в компьютерных системах от несанкционированного доступа	4
35	Методы и средства защиты от несанкционированного изменения структур компьютерных систем	4
36	Криптографические методы защиты информации	4
37	Криптология, криптография и криптоанализ	4
38	Классификация криптографических методов	4
39	Симметричное и асимметричное шифрование	4
40	Электронная подпись	4
41	Особенности защиты информации в распределенных компьютерных системах	4
41	Характеристика угроз ИБ в распределенных компьютерных системах	4
23	Защита информации в каналах связи	4
44	Межсетевое экранирование	4
45	Подтверждение подлинности информации и взаимодействующих процессов	4
46	Практические рекомендации пользователям глобальной сети Интернет по обеспечению информационной безопасности	4
47	Классификация компьютерных вирусов и вредоносных программ	4
48	Файловые, загрузочные и сетевые вирусы	4
49	Методы и средства борьбы с вирусами и вредоносными программами	4
50	Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения	4

Приложение Б. Тестовые задания к зачёту

1. Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 5.12. 2016 №649, служит основой для …

а) выполнения всех приведенных мероприятий;

б) формирования государственной политики в области обеспечения ИБ РФ;

в) подготовки предложений по совершенствованию правового и методического обеспечения ИБ РФ;

г) подготовки предложений по совершенствованию научно-технического и организационного обеспечения ИБ РФ;

д) разработки целевых программ обеспечения ИБ РФ.

2. Состояние защищенности ее национальных интересов РФ в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства называют …

а) информационной безопасностью;

б) защитой интересов государства в информационной сфере;

в) защитой интересов общества в информационной сфере;

г) защитой интересов личности в информационной сфере;

д) защитой информации.

3. Согласно определению ИБ прописанному в Доктрине информационной безопасности РФ, интересы личности в информационной сфере заключаются …

а) все перечисленное определяет интересы личности в информационной сфере;

б) в реализации конституционных прав человека и гражданина на доступ к информации;

в) в реализации конституционных прав человека и гражданина на использование информации в интересах осуществления не запрещенной законом деятельности;

г) в реализации конституционных прав человека и гражданина на использование информации в интересах физического, духовного и интеллектуального развития;

д) в защите информации, обеспечивающей личную безопасность.

4. Согласно Доктрине информационной безопасности РФ,

интересы общества в информационной сфере заключаются …

а) все перечисленное определяет интересы общества в информационной сфере;

б) в обеспечении интересов личности в этой сфере;

в) в упрочении демократии, создании правового социального государства;

г) в достижении и поддержании общественного согласия;

д) в духовном обновлении России.

5. Согласно Доктрине информационной безопасности РФ, интересы государства в информационной сфере реализуются в целях …

а) все перечисленное определяет интересы государства в информационной сфере;

б) обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России;

в) обеспечения политической, экономической и социальной стабильности;

г) в безусловном обеспечении законности и правопорядка;

д) в развитии равноправного и взаимовыгодного международного сотрудничества.

6. Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации, это …

а) источник угрозы безопасности информации;

б) фактор, воздействующий на защищаемую информацию;

в) уязвимость информационной системы;

г) несанкционированное воздействие на информацию;

д) угроза безопасности информации.

7. Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации, это …

а) объект защиты информации;

б) защищаемая информация;

в) носитель защищаемой информации;

г) защищаемый объект информатизации;

д) защищаемая информационная система.

8. Основная идея, раскрывающая состав, содержание,

взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации , это …

а) замысел защиты информации;

б) цель защиты информации;

в) система защиты информации;

г) политика безопасности (информации в организации) ;

д) безопасность информации (данных).

9. Порядок и правила применения определенных принципов и средств защиты информации это …

а) способ защиты информации;

б) защита информации от утечки;

в) защита информации от несанкционированного воздействия;

г) защита информации от непреднамеренного воздействия;

д) защита информации от несанкционированного доступа.

10. Согласно Стратегии национальной безопасности РФ до 2020 года важнейшими задачами в области обеспечения информационной безопасности РФ являются:

а) все перечисленные задачи являются важнейшими;

б) реализация конституционных прав и свобод граждан России в сфере информационной деятельности;

в) совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;

г) противодействие угрозе развязывания противоборства в информационной сфере;

д) все перечисленные задачи являются второстепенными.

11. Национальные интересы РФ в информационной сфере и их обеспечение, виды угроз и источники угроз информационной безопасности (ИБ) РФ, а также состояние ИБ РФ и основные задачи и методы по ее обеспечению определены …

а) в Доктрине информационной безопасности РФ, утвержденной Указом Президента РФ от 5.12. 2016 №649;

б) в Стратегии национальной безопасности РФ до 2020 года, утвержденной Указом Президента РФ от 12.05.2009 №537;

в) в Военной доктрине РФ, утверждённой Указом Президента РФ от 05.02.2010 №146;

г) в Федеральном законе от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

д) в Постановлении Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации».

12. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

а) выполнение всех перечисленных мероприятий;

б) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения;

в) обеспечение защиты информации от иных неправомерных действий в отношении такой информации;

г) соблюдение конфиденциальности информации ограниченного доступа

д) реализацию права на доступ к информации.

13. Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

а) все перечисленные могут являться угрозами;

б) противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

в) неисполнение всеми органами власти, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;

г) неправомерное ограничение доступа граждан к открытым информационным ресурсам всех органов власти к открытым архивным материалам, к другой открытой социально значимой информации;

д) дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы.

14. Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

а) все перечисленные могут являться угрозами;

б) нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

в) вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка;

г) усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

д) девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе.

15. Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, могут являться:

а) все перечисленные могут являться угрозами;

б) противодействие доступу РФ к новейшим информационным технологиям;

в) противодействие доступу к взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг;

г) противодействие доступу к взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии средств информатизации, телекоммуникации и связи, информационных продуктов;

д) создание условий для усиления технологической зависимости России в области современных информационных технологий.

16. Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

а) все перечисленные могут являться угрозами;

б) использование несертифицированных отечественных и зарубежных ИТ, средств защиты информации, средств информатизации, телекоммуникации и связи;

в) несанкционированный доступ к информации, находящейся в банках и базах данных;

г) перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

д) нарушение законных ограничений на распространение информации.

17. Согласно Доктрине информационной безопасности РФ к источникам внешних угроз НЕ относятся:

а) все перечисленные относятся к внешним угрозам ИБ РФ;

б) деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере;

в) стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве;

г) стремление ряда стран к вытеснению России с внешнего и внутреннего информационных рынков;

д) обострение международной конкуренции за обладание информационными технологиями и ресурсами.

18. Согласно Доктрине информационной безопасности РФ к источникам внешних угроз НЕ относятся:

а) все перечисленные относятся к внешним угрозам ИБ РФ;

б) деятельность международных террористических организаций;

в) увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию создания конкурентоспособных российских информационных технологий;

г) деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

д) разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира.

19. По своей общей направленности к угрозам информационной безопасности РФ НЕ относятся следующие виды:

а) все перечисленные относятся к угрозам информационной безопасности РФ;

б) угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной

деятельности;

в) угрозы индивидуальному, групповому и общественному сознанию, духовному возрождению России;

г) угрозы информационному обеспечению государственной политики Российской Федерации;

д) угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи.

20. К какому из перечисленных видов информации согласно закону может быть ограничен доступ?

а) ко всем перечисленным видам информации законом запрещёно ограничение доступа;

б) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

в) информации о состоянии окружающей среды;

г) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

д) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией.

21. Прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации, это …

а) оценка соответствия требованиям по защите информации;

б) лицензирование в области защиты информации;

в) сертификация на соответствие требованиям по безопасности информации;

г) мониторинг безопасности информации;

д) экспертиза документа по защите информации.

22. Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или

используемые для защиты информации, это …

а) средство защиты информации;

б) техника защиты информации;

в) средство контроля эффективности защиты информации;

г) средство физической защиты информации;

д) криптографическое средство защиты информации.

23. Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств это ...

а) техническая защита информации;

б) правовая защита информации;

в) организационная защита информации;

г) физическая защита информации;

д) криптографическая защита информации.

24. Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты это…

а) физическая защита информации;

б) криптографическая защита информации;

в) техническая защита информации;

г) правовая защита информации;

д) организационная защита информации.

25. Согласно Доктрине информационной безопасности РФ к источникам внешних угроз НЕ относятся:

а) все перечисленные относятся к внешним угрозам ИБ РФ;

б) деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

в) разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира;

г) разработка рядом государств концепций информационных войн, предусматривающих нарушение нормального функционирования информационных и телекоммуникационных

систем РФ;

д) разработка рядом государств концепций информационных войн, предусматривающих нарушение сохранности информационных ресурсов, получение несанкционированного доступа к ним.

26. Политика безопасности и комплекс процедур по безопасности информационной среды формируется на…

а) законодательном уровне;

б) административном уровне;

в) программно-техническом уровне;

г) пользовательском уровне;

д) на всех перечисленных уровнях.

27. Согласно Доктрине информационной безопасности РФ к источникам внутренних угроз НЕ относятся:

а) все перечисленные относятся к внутренним угрозам ИБ РФ;

б) критическое состояние отечественных отраслей промышленности;

в) неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере;

г) получение криминальными структурами доступа к конфиденциальной информации;

д) усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере.

28. Согласно Доктрине информационной безопасности РФ к источникам внутренних угроз НЕ относятся:

а) все перечисленные относятся к внутренним угрозам ИБ РФ;

б) недостаточная координация деятельности всех органов власти по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ;

в) недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

г) неразвитость институтов гражданского общества и недостаточный государственный контроль над развитием

информационного рынка России;

д) недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ.

29. Согласно Доктрине информационной безопасности РФ к источникам внутренних угроз НЕ относятся:

а) все перечисленные относятся к внутренним угрозам ИБ РФ;

б) недостаточная экономическая мощь государства;

в) снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

г) недостаточная активность всех органов власти в информировании общества о своей деятельности, разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развития системы доступа к ним граждан;

д) отставание России от ведущих стран мира по уровню информатизации всех органов власти, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

30. Доктрина определяет в качестве общих методов обеспечения информационной безопасности РФ:

а) правовые, организационно-технические и экономические;

б) правовые, организационно-методические и экономические;

в) правовые, организационно-политические и экономические;

г) правовые, научно-технические и экономические;

д) правовые, организационно-политические и научно-экономические.

31. Наиболее важным направлением реализации правовых методов обеспечения ИБ РФ является внесение изменений и дополнений в законодательство РФ в целях …

а) все перечисленные относятся к данному направлению реализации правовых методов обеспечения ИБ РФ;

б) создания и совершенствования системы обеспечения ИБ РФ;

в) устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, к которым присоединилась РФ;

г) устранения противоречий между федеральными законодательными актами и законодательными актами субъектов

РФ;

д) конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения ИБ РФ.

32. Реализация правовых методов обеспечения ИБ РФ предполагает разработку и принятие НПА РФ, устанавливающих ответственность юридических и физических лиц …

а) за все перечисленные противоправные деяния;

б) за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование;

в) за преднамеренное распространение недостоверной информации;

г) за противоправное раскрытие конфиденциальной информации;

д) за использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну.

33. Организационно-техническими методами обеспечения информационной безопасности РФ являются:

а) все перечисленные методы;

б) создание и совершенствование системы обеспечения ИБ РФ;

в) усиление правоприменительной деятельности органов исполнительной власти включая предупреждение и пресечение правонарушений в информационной сфере;

г) усиление правоприменительной деятельности органов исполнительной власти, включая выявление, изобличение и привлечение к ответственности лиц, совершивших преступление и другие правонарушения в этой сфере;

д) разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств.

34. Организационно-техническими методами обеспечения информационной безопасности РФ являются:

а) все перечисленные методы;

б) развитие защищенных телекоммуникационных систем;

в) повышение надежности специального программного обеспечения;

г) создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации;

д) создание систем и средств предотвращения специальных воздействий, вызывающих разрушение, уничтожение, искажение информации.

35. Организационно-техническими методами обеспечения информационной безопасности РФ являются:

а) все перечисленные методы;

б) создание систем и средств предотвращения изменения штатных режимов функционирования систем и средств информатизации и связи;

в) выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем;

г) предотвращение перехвата по техническим каналам;

д) применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи.

36. Организационно-техническими методами обеспечения информационной безопасности РФ являются:

а) все перечисленные методы;

б) контроль за выполнением специальных требований по защите информации;

в) сертификация средств защиты информации;

г) лицензирование деятельности в области защиты государственной тайны;

д) стандартизация способов и средств защиты информации.

37. Организационно-техническими методами обеспечения информационной безопасности РФ являются:

а) все перечисленные методы;

б) совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;

в) контроль за действиями персонала в защищенных информационных системах;

г) подготовка кадров в области обеспечения информационной

безопасности РФ;

д) формирование системы мониторинга показателей и характеристик информационной безопасности РФ в наиболее важных сферах и деятельности общества и государства.

38. Экономические методы обеспечения информационной безопасности РФ включают:

а) всё перечисленное;

б) разработку программ обеспечения ИБ РФ;

в) определение порядка финансирования программ обеспечения ИБ РФ;

г) совершенствование системы финансирование работ, связанных с реализацией правовых и организационно-технических методов защиты информации;

д) создание системы страхования информационных рисков физических и юридических лиц.

39. Основными составляющими в интенсификации информационных процессов при системно-кибернетическом и социальном подходе к формализации хода общественного развития являются:

а) все перечисленные факторы;

б) увеличение объема добываемой и передаваемой информации;

в) расширение наглядного (визуального) представления информации в процессах управления;

г) бурный рост технической оснащенности управленческого труда;

д) учет особенностей социально-психологических взаимодействий человеческого социума и образований.

40. Воздействию угроз информационной безопасности РФ в сфере экономики наиболее подвержены:

а) все перечисленные системы;

б) система государственной статистики и кредитно-финансовая система;

в) информационные и учетные автоматизированные системы подразделений ФОИВ, обеспечивающих деятельность общества и государства в сфере экономики;

г) системы бухгалтерского учета предприятий, учреждений и

организаций независимо от формы собственности;

д) системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности.

41. Что из перечисленного НЕ должна делать антивирусная программа?

а) антивирусная программа должна делать всё перечисленное;

б) проверять системные области на загрузочном диске при включении компьютера;

в) проверять файлы на установленных в ПК сменных носителях;

г) предоставлять возможность выбора графика периодичности проверки жесткого диска;

д) автоматически проверять загружаемые файлы.

42. Что из перечисленного НЕ должна делать антивирусная программа?

а) антивирусная программа должна делать всё перечисленное;

б) проверять системные области на загрузочном диске при включении компьютера;

в) автоматически проверять загружаемые файлы;

г) проверять исполняемые файлы перед их запуском;

д) обеспечивать возможность обновления версии через Интернет.

43. Обмениваясь файлами с другими пользователями, особенно загружаемых вами из сети Интернет или приложенных к электронным посланиям рекомендуется …

а) сразу проверять все входящие файлы (документы, программы) на наличие вируса;

б) проверять все входящие файлы (документы, программы) на наличие вируса в течение первого часа, после обмена файлами;

в) проверять все входящие файлы (документы, программы) на наличие вируса не позднее 24 часов после обмена файлами;

г) проверять все входящие файлы (документы, программы) на наличие вируса не позднее одной недели после обмена файлами;

д) проверять все входящие файлы (документы, программы) на наличие вируса не обязательно.

44. Делайте резервные копии своих данных. Это поможет …

а) восстановить информацию в случае воздействия вируса, сбоя в системе или выхода из строя жесткого диска;

б) восстановить информацию в случае воздействия вируса или выхода из строя жесткого диска;

в) восстановить информацию в случае сбоя в системе или выхода из строя жесткого диска;

г) восстановить информацию в случае воздействия вируса и сбоя в системе;

д) восстановить информацию в случае выхода из строя жесткого диска.

45. Проверять на наличие вирусов старые файлы и диски нужно, потому что …

а) все перечисленные факторы имеют место;

б) обычные вирусы, равно как и макровирусы, пробуждаются только в тот момент, когда вы открываете или загружаете инфицированный файл;

в) вирусы могут долгое время незаметно храниться на жестком диске в зараженных программах и файлах данных;

г) вирусы могут долгое время незаметно храниться на жестком диске в приложениях к непрочитанным электронным письмам;

д) вирусы могут долгое время незаметно храниться на жестком диске в сжатых файлах.

46. Какие из приведенных советов не влияют на защиту данных?

а) все советы полезные;

б) установите пароли на BIOS и на экранную заставку;

в) исключите доступ посторонних лиц к вашему компьютеру;

г) создайте аварийную загрузочную дискету;

д) систематически делайте резервное копирование данных.

47. Какие из приведенных советов не влияют на защиту данных?

а) все советы полезные;

б) регулярно очищайте Корзину с удаленными файлами;

в) проводите архивацию файлов и устанавливайте пароли на файлы с важной информацией;

г) при установке пароля не используйте ваше имя, фамилию, телефон;

д) после удаления большого количества файлов, но не реже одного раза в месяц, производите дефрагментацию жесткого диска.

48. Обеспечение готовности системы к обслуживанию поступающих к ней запросов это критерий …

а) доступности информации;

б) целостности информации;

в) конфиденциальности информации;

г) закрытости информации;

д) открытости информации.

49. Обеспечение существования информации в неискаженном виде это критерий …

а) целостности информации;

б) конфиденциальности информации;

в) закрытости информации;

г) открытости информации;

д) доступности информации.

50. Обеспечение доступа к информации только авторизованному кругу субъектов это критерий …

а) конфиденциальности информации;

б) закрытости информации;

в) открытости информации;

г) доступности информации;

д) целостности информации.

51. При включении информационных ресурсов в трансграничные информационные сети, в первую очередь Интернет, должны защищаться:

а) все перечисленные информационные ресурсы и услуги;

б) информационные ресурсы на всех видах носителей, в том числе содержащие информацию ограниченного доступа;

в) информационные системы и их сети;

г) информационные технологии и средства их обеспечения;

д) машинные носители с информацией, например, средствами электронной цифровой подписи или криптографии.

52. При включении информационных ресурсов в трансграничные информационные сети, в первую очередь Интернет, должны защищаться:

а) все перечисленные информационные ресурсы и услуги;

б) информационные технологии и средства их обеспечения;

в) машинные носители с информацией, например, средствами электронной цифровой подписи или криптографии;

г) базы данных (знаний) в составе автоматизированных информационных систем и их сетей;

д) программные средства в составе электронных вычислительных машин (ЭВМ), их сетей.

53. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации, называется …

а) защищаемая информация;

б) секретная информация;

в) совершенно секретная информация;

г) информация особой важности;

д) информация для служебного пользования.

54. Собственником информации может быть …

а) любой из перечисленных субъектов;

б) государство;

в) юридическое лицо;

г) группа физических лиц;

д) отдельное физическое лицо.

55. Деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, это …

а) защита информации;

б) сохранение информации;

в) охрана информации;

г) хранение информации;

д) защита от утечки информации.

56. Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации (иностранными) разведками, это …

а) защита информации от утечки;

б) защита информации от несанкционированного воздействия;

в) защита информации от непреднамеренного воздействия;

г) защита информации от разглашения;

д) защита информации от несанкционированного доступа.

57. Деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации, это …

а) защита информации от несанкционированного воздействия;

б) защита информации от непреднамеренного воздействия;

в) защита информации от разглашения;

г) защита информации от несанкционированного доступа;

д) защита информации от разведки.

58. Деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, это …

а) защита информации от непреднамеренного воздействия;

б) защита информации от разглашения;

в) защита информации от несанкционированного доступа;

г) защита информации от разведки;

д) защита информации от несанкционированного воздействия.

59. Деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации, это …

а) защита информации от разглашения;

б) защита информации от несанкционированного доступа;

в) защита информации от разведки;

г) защита информации от несанкционированного воздействия;

д) защита информации от непреднамеренного воздействия.

60. Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правил доступа к защищаемой информации, это …

а) защита информации от несанкционированного доступа;

б) защита информации от разведки;

в) защита информации от несанкционированного воздействия;

г) защита информации от непреднамеренного воздействия;

д) защита информации от разглашения.

61. Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать:

а) любой из перечисленных субъектов;

б) государство;

в) юридическое лицо;

г) группа физических лиц, в том числе общественная организация;

д) отдельное физическое лицо.

62. Деятельность по предотвращению получения защищаемой информации разведкой, это …

а) защита информации от разведки;

б) защита информации от технической разведки;

в) защита информации от агентурной разведки;

г) защита информации от военной разведки;

д) защита информации от космической разведки.

63. Деятельность по предотвращению получения защищаемой информации разведкой с помощью технических средств, это …

а) защита информации от технической разведки;

б) защита информации от агентурной разведки;

в) защита информации от военной разведки;

г) защита информации от космической разведки;

д) защита информации от финансовой разведки.

64. Целью защиты информации может быть предотвращение ущерба в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию …

а) собственнику, владельцу, пользователю информации;

б) собственнику, разработчику, пользователю информации;

в) собственнику, автору, пользователю информации;

г) государству, владельцу, пользователю информации;

д) обществу, владельцу, пользователю информации.

65. Эффективность защиты информации, это …

а) степень соответствия результатов защиты информации

поставленной цели;

б) мера или характеристика для оценки эффективности защиты информации;

в) значения показателей эффективности защиты информации, установленные нормативными документами;

г) совокупность действий по разработке и/или практическому применению способов и средств защиты информации;

д) все перечисленные показатели в комплексе.

66. Показатель эффективности защиты информации, это …

а) мера или характеристика для оценки эффективности защиты информации;

б) значения показателей эффективности защиты информации, установленные нормативными документами;

в) совокупность действий по разработке и/или практическому применению способов и средств защиты информации;

г) степень соответствия результатов защиты информации поставленной цели;

д) все перечисленные показатели в комплексе.

67. Нормы эффективности защиты информации, это …

а) значения показателей эффективности защиты информации, установленные нормативными документами;

б) совокупность действий по разработке и/или практическому применению способов и средств защиты информации;

в) степень соответствия результатов защиты информации поставленной цели;

г) мера или характеристика для оценки эффективности защиты информации;

д) все перечисленные показатели в комплексе.

68. Организация защиты информации, это …

а) содержание и порядок действий по обеспечению защиты информации;

б) степень соответствия результатов защиты информации поставленной цели;

в) мера или характеристика для оценки эффективности защиты информации;

г) значения показателей эффективности защиты информации, установленные нормативными документами;

д) совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

69. Совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также организованные и функционирующие по соответствующим правилам объекты защиты, это …

а) система защиты информации;

б) организация защиты информации;

в) мероприятие по защите информации;

г) техника защиты информации;

д) все определения верны.

70. Совокупность действий по разработке и/или практическому применению способов и средств защиты информации, это …

а) мероприятие по защите информации;

б) техника защиты информации;

в) система защиты информации;

г) организация защиты информации;

д) все определения верны.

71. Совокупность действий по разработке и/или практическому применению методов (способов) и средств контроля эффективности защиты информации, это …

а) мероприятие по контролю эффективности защиты информации;

б) мероприятие по защите информации;

в) техника защиты информации;

г) система защиты информации;

д) организация защиты информации.

72. Средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации, это …

а) техника защиты информации;

б) система защиты информации;

в) организация защиты информации;

г) мероприятие по контролю эффективности защиты информации;

д) мероприятие по защите информации.

73. Информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации, это …

а) объект защиты информации;

б) способ защиты информации;

в) метод защиты информации;

г) контроль защиты информации;

д) средство защиты информации.

74. Порядок и правила применения определенных принципов и средств защиты информации, это …

а) способ защиты информации;

б) метод защиты информации;

в) контроль защиты информации;

г) средство защиты информации;

д) объект защиты информации.

75. Установление градаций важности защиты защищаемой информации (объекта защиты), это …

а) категорирование защищаемой информации (объекта защиты);

б) иерархирование защищаемой информации (объекта защиты);

в) документирование защищаемой информации (объекта защиты);

г) архивирование защищаемой информации (объекта защиты);

д) систематизация защищаемой информации (объекта защиты).

76. Порядок и правила применения определенных принципов и средств контроля эффективности защиты информации, это …

а) метод (способ) контроля эффективности защиты информации;

б) система контроля эффективности защиты информации;

в) элементы контроля эффективности защиты информации;

г) средство контроля эффективности защиты информации;

д) объекты контроля эффективности защиты информации.

77. Проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации, это ...

а) контроль состояния защиты информации;

б) контроль состояния системы информации;

в) методика контроля состояния защиты информации;

г) система контроля состояния защиты информации;

д) контроль результатов защиты информации.

78. Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации, это …

а) средство защиты информации;

б) способ защиты информации;

в) объект защиты информации;

г) метод защиты информации;

д) контроль защиты информации.

79. Техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации, это ...

а) средство контроля эффективности защиты информации;

б) метод контроля эффективности защиты информации;

в) объект контроля эффективности защиты информации;

г) способ контроля эффективности защиты информации;

д) субъект контроля эффективности защиты информации.

80. Проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации, это ...

а) контроль организации защиты информации;

б) контроль эффективности защиты информации;

в) организационный контроль эффективности защиты информации;

г) технический контроль эффективности защиты информации;

д) общественный контроль эффективности защиты информации.

81. Проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации, это ...

а) контроль эффективности защиты информации;

б) организационный контроль эффективности защиты

информации;

в) технический контроль эффективности защиты информации;

г) общественный контроль эффективности защиты информации;

д) контроль организации защиты информации.

82. Проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации, это …

а) организационный контроль эффективности защиты информации;

б) технический контроль эффективности защиты информации;

в) общественный контроль эффективности защиты информации;

г) контроль организации защиты информации;

д) контроль эффективности защиты информации;

83. Контроль эффективности защиты информации, проводимой с использованием средств контроля, это …

а) технический контроль эффективности защиты информации;

б) общественный контроль эффективности защиты информации;

в) контроль организации защиты информации;

г) контроль эффективности защиты информации;

д) организационный контроль эффективности защиты информации.

84. Из перечисленных нарушений НЕ относятся к основным группам причин сбоев и отказов в работе компьютерных систем:

а) все перечисленные относятся;

б) нарушения физической и логической целостности хранящихся в оперативной и внешней памяти структур данных, возникающие по причине старения или преждевременного износа их носителей;

в) нарушения, возникающие в работе аппаратных средств из-за их старения или преждевременного износа;

г) нарушения физической и логической целостности хранящихся в оперативной и внешней памяти структур данных, возникающие по причине некорректного использования компьютерных ресурсов;

д) нарушения, возникающие в работе аппаратных средств из-за неправильного использования или повреждения, в том числе из-за неправильного использования программных средств.

85. Специальные способы защиты информации от нарушений работоспособности компьютерных систем, это …

а) все перечисленные относятся к специальным способам;

б) внесение структурной и временной избыточности компьютерных ресурсов;

в) внесение информационной и функциональной избыточности компьютерных ресурсов;

г) защиту от некорректного использования ресурсов компьютерной системы;

д) выявление и своевременное устранение ошибок на этапах разработки программно-аппаратных средств.

86. За счет резервирования аппаратных компонентов и машинных носителей данных, организации замены отказавших и своевременного пополнения резервных компонентов достигается …

а) структурная избыточность компьютерных ресурсов;

б) информационная избыточность компьютерных ресурсов;

в) временная избыточность компьютерных ресурсов;

г) функциональная избыточность компьютерных ресурсов;

д) защита от некорректного использования компьютерных ресурсов.

87. Путем периодического или постоянного (фонового) резервирования данных на основных и резервных носителях выполняется ...

а) временная избыточность компьютерных ресурсов;

б) функциональная избыточность компьютерных ресурсов;

в) защита от некорректного использования компьютерных ресурсов;

г) структурная избыточность компьютерных ресурсов;

д) информационная избыточность компьютерных ресурсов.

88. Путём дублированием функций или внесением дополнительных функций в программно-аппаратные ресурсы вычислительной системы для повышения ее защищенности от сбоев и отказов достигается …

а) функциональная избыточность компьютерных ресурсов;

б) защита от некорректного использования компьютерных ресурсов;

в) структурная избыточность компьютерных ресурсов;

г) информационная избыточность компьютерных ресурсов;

д) временная избыточность компьютерных ресурсов.

89. В корректном функционировании программного обеспечения с позиции использования ресурсов вычислительной системы заключается …

а) защита от некорректного использования компьютерных ресурсов;

б) структурная избыточность компьютерных ресурсов;

в) информационная избыточность компьютерных ресурсов;

г) временная избыточность компьютерных ресурсов;

д) функциональная избыточность компьютерных ресурсов.

90. Путем качественного выполнения базовых стадий разработки на основе системного анализа концепции, проектирования и реализации проекта достигается …

а) выявление и устранение ошибок при разработке программно-аппаратных средств;

б) структурная избыточность компьютерных ресурсов;

в) информационная избыточность компьютерных ресурсов;

г) временная избыточность компьютерных ресурсов;

д) функциональная избыточность компьютерных ресурсов.

91. Задачами по защите от угроз целостности и конфиденциальности информации являются …

а) все перечисленные;

б) запрещение несанкционированного доступа к ресурсам вычислительных систем;

в) невозможность несанкционированного использования компьютерных ресурсов при осуществлении доступа;

г) своевременное обнаружение факта несанкционированных действий;

д) своевременное устранение причин и последствий несанкционированных действий.

92. Наиболее распространенными способами разграничения доступа являются:

а) все перечисленные способы являются распространёнными;

б) разграничение по спискам (пользователей или ресурсов)

в) использование матрицы установления полномочий (строки матрицы – идентификаторы пользователей, столбцы – ресурсы компьютерной системы) ;

г) разграничение по уровням секретности и категориям (например, общий доступ, конфиденциально, секретно);

д) парольное разграничение.

93. Обратимое преобразование некоторого понятного исходного текста (открытого текста) в кажущуюся случайной последовательность некоторых знаков, называют …

а) шифротекстом или криптограммой;

б) шифротекстом или голограммой;

в) криптотекстом или криптограммой;

г) криптотекстом или шифрограммой;

д) шифротекстом или шифрограммой.

94. Одной из основных угроз хищения информации является угроза доступа к остаточным данным, оставшимся в освободившихся участках оперативной и внешней памяти компьютера …

а) после любого из перечисленных действий;

б) после удаления файлов пользователя;

в) после удаления временных файлов без ведома пользователя, находящиеся в неиспользуемых хвостовых частях последних кластеров, занимаемых файлами;

г) в кластерах, освобожденных после уменьшения размеров файлов;

д) в кластерах, освобожденных после форматирования дисков.

95. Информационным оружием называются средства:

а) все перечисленные средства относятся к информационному оружию;

б) уничтожения, искажения или хищения информационных массивов;

в) преодоления систем защиты;

г) ограничения допуска законных пользователей;

д) дезорганизация работы технических средств, компьютерных систем.

96. Атакующим информационным оружием сегодня можно

назвать:

а) всё перечисленное является атакующим информационным оружием;

б) компьютерные вирусы, способные размножаться, внедряться в программы, передаваться по линиям связи, сетям передачи данных, выводить из строя системы управления и т.д. ;

в) логические бомбы – программные закладные устройства, которые заранее внедряют в информационно-управляющие центры военной или гражданской инфраструктуры, чтобы по сигналу или в установленное время привести их в действие;

г) средства подавления информационного обмена в телекоммуникационных сетях, фальсификация информации в каналах государственного и военного управления;

д) различного рода ошибки, сознательно вводимые противником в программное обеспечение объекта.

97. В соответствии с Доктриной информационной безопасности РФ, основным направлением международного сотрудничества должно стать …

а) запрещение разработки, распространения и применения информационного оружия;

б) реализация принципа ответственности государств за свои национальные сегменты сети Интернет, в том числе за содержание размещаемой в них информации;

в) выработка единых подходов к вопросу прекращения работы Интернет-сайтов тер-рористического и экстремистского характера;

г) обмен информацией о признаках, фактах, методах и средствах использования сети Интернет в террористических целях;

д) обмен информацией об устремлениях и деятельности террористических организаций в сфере IT-технологий.

98. Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа) – это …

а) аутентификация;

б) верификация;

в) дешифрование;

г) декодирование;

д) криптография.

99. Представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д. – это …

а) кодирование информации;
б) линейное шифрование;
в) верификация;
г) аутентификация;
д) идентификация.

100. Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации, это …

а) угроза безопасности информации;
б) фактор, воздействующий на защищаемую информацию;
в) источник угрозы безопасности информации;
г) уязвимость информационной системы;
д) несанкционированное воздействие на информацию.

Приложение В. Правила визуализации информации

Под визуализацией учебного материала понимается представление, структурирование и оформление учебных знаний в наглядной форме с помощью рисунков, графиков и анимации.

Умение и владение правилами визуализации учебной информации характеризуют уровень владения обучающимися информационной компетентностью, благодаря которой формируются умения самостоятельно искать, анализировать и отбирать необходимую информацию, организовывать, преобразовывать, сохранять и передавать её с помощью информационных технологий.

Приведенные в данном приложении правила визуализации информации, использования цвета и логических ударений рекомендуются к использованию при разработке рефератов-презентаций в объеме комплексных заданий по темам №1, 8 и 9.

А). Закономерности и правила визуализации информации

Правило 1. Вертикальная линия считывается дольше, чем горизонтальная, хотя они равны по величине. Отсюда следует, что и

текст, напечатанный в столбик, считывается медленнее, чем этот же текст, напечатанный более широким планом.

Правило 2. Линии, не имеющие перерыва, с плавными закруглениями считываются дольше, чем линия с резко выраженными углами, следовательно, печатный текст будет читаться быстрее, чем письменный, даже если почерк разборчивый.

Правило 3. Зрение требует группировки информации. Психологи утверждают, что вертикально нужно давать нечетное число перечислений: 3, 5, 7. Наибольшее число вертикальных перечислений, которое запоминает человек, – это 7±2 (имен, наименований). Четное число вертикально записанных перечислений запоминается хуже.

Правило 4. Величина букв на слайде влияет на комфортность восприятия визуальной информации. Существуют понятия комфортного зрения и предельного зрения. Так, при величине букв в 1 см предельное зрение равно 3 метра, а комфортное – 2 метра.

Правило 5. Лучше всего запоминается информация, расположенная на слайде в правом верхнем углу – 33 % внимания подается туда. Левому верхнему углу «уделяется» 28% внимания, правому нижнему 23% и левому нижнему 16 %.

Правило 6. Восприятие считываемой информации зависит от удобочитаемости текста, то есть играют роль не только рисунок и размер шрифта, но и различное соотношение материала, расположение на слайде (длина строки, междустрочия, межбуквенные пробелы, характер верстки текста), цвет фона, способ печати.

Правило 7. Чем короче, компактней и выразительней текст, тем больше шансов, что его прочтут и запомнят. Это же относится и к заголовкам. Оптимально для заголовка использовать от 3 до 7 слов.

Правило 8. При подборе ключевых положений, полезно учитывать следующее: в единицу времени лучше всего запоминаются группы слов (78%), затем предложения (37%), далее следуют отдельные слова (25%), слоги (11%), и буквы (7%). Исходя из этого, буквенные сокращения в опорных конспектах должны быть ограничены. В экстремальных условиях лучше запоминаются слова, чем цифры. В русском языке существительные запоминаются лучше, чем глаголы и прилагательные.

Правило 9. При разработке формата кадра на экране и его построении целесообразно учитывать, что существуют смысл и отношение между объектами, которые определяют организацию зрительного поля.

Правило 10. Компоновать объекты на слайде рекомендуется близко друг от друга, так как чем ближе в зрительном поле объекты друг к другу (при прочих равных условиях), тем с большей вероятностью они организуются в единые, целостные образы.

Правило 11. Компоновать объекты на слайде рекомендуется с учетом свойств продолжения, так как, чем больше элементы в зрительном поле оказываются в местах, соответствующих продолжению закономерной последовательности (функционируют как части знакомых контуров), тем с большей вероятностью они организуются в целостные единые образы.

Правило 12. Компоновать объекты на слайде рекомендуется таким образом, чтобы они образовывали замкнутые цепи, так как чем больше элементы зрительного поля образуют замкнутые цепи, тем с большей готовностью они будут организовываться в отдельные образы.

Правило 13. Компоновать объекты на слайде рекомендуется с учетом особенности выделения предмета и фона при выборе формы объектов, размеров букв и цифр, насыщенности цвета, расположения текста и т.п.

Правило 14. При компоновке объектов на слайде рекомендуется не перегружать визуальную информацию деталями, яркими и контрастными цветами.

Правило 15. При компоновке объектов на слайде рекомендуется выделять учебный материал, предназначенный для запоминания цветом, подчеркиванием, размером шрифта и т.п.

Б). Основные правила использования цвета

Правило 1. Не использовать более трех-четырех цветов на одном листе, обеспечивать хороший контраст фигур (опорных сигналов) и фона, иллюстрировать одним цветом одинаковые положения, признаки понятий.

Правило 2. Использовать цветовые ассоциации и эмоциональные характеристики, например, красным или оранжевым

выделять указания, требующие обязательного выполнения, а черным – отрицательные или негативные последствия.

Правило 3. При разработке и формировании слайдов презентации необходимо учитывать, что объекты, изображенные разными цветами и на разном фоне, по-разному воспринимаются человеком. Если яркость цвета объектов и яркость фона значительно отличаются от кривой относительной видности, то при поверхностном рассмотрении изображения может возникнуть эффект «психологического пятна», когда некоторые объекты как бы выпадают из поля зрения. При более внимательном рассмотрении изображения восприятие этих объектов требует дополнительных зрительных усилий.

Правило 4. Важную роль в организации зрительной информации играет контраст предметов по отношению к фону. Существует две разновидности контраста: прямой и обратный. При прямом контрасте предметы и их изображения темнее, а при обратном - светлее фона. В компонентах презентации целесообразно использовать оба вида, как порознь в разных кадрах, так и вместе в рамках одной картинки.

Правило 5. Из психологии следует, что предпочтительной является работа в прямом контрасте. В этих условиях увеличение яркости ведет к улучшению видимости, а при обратном – к ухудшению, но цифры, буквы и знаки, предъявляемые в обратном контрасте, опознаются точнее и быстрее, чем в прямом даже при меньших размерах.

Правило 6. Чем больше относительные размеры частей изображения и выше его яркость, тем меньший должен быть контраст, тем лучше видимость. При разработке презентаций следует помнить, что комфортность восприятия информации с экрана монитора достигается при равномерном распределении яркости в поле зрения.

Правило 7. Соотношение цветов в цветовой палитре информационного ресурса может формировать определенный психологический настрой пользователей презентаций. Преобладание темных цветов может привести к развитию угнетенного психологического состояния, пассивности. Преобладание ярких цветов, наоборот, - к перевозбуждению, причем общее перевозбуждение организма часто граничит с быстрым развитием утомления зрительного анализатора.

Правило 8. Значения цветов рекомендуется устанавливать постоянными и соответствующими устойчивым зрительным ассоциациям, реальным предметам и объектам. Кроме того, значения цветов рекомендуется выбирать в соответствии с психологической реакцией человека (например, красный цвет – прерывание, экстренная информация, опасность, желтый – внимание и слежение, зеленый – разрешающий и т.д.). Для смыслового противопоставления объектов (данных) рекомендуется использование в презентациях контрастных цветов (красный-зеленый, синий-желтый, белый-черный).

Правило 9. При создании слайдов презентации не рекомендуется злоупотребление контрастными цветами, поскольку это часто приводит к появлению психологических послеобразов и цветовых гомогенных полей. Цветовой контраст изображения и фона должен находиться на оптимальном уровне, яркостный контраст изображения по отношению к фону должен быть выше не менее, чем на 60%.

Правило 10. Необходимо учитывать, что красный цвет обеспечивает благоприятные условия восприятия только при высокой яркости изображения, зеленый в среднем диапазоне яркости, желтый – в широком диапазоне уровней яркости изображения, синий – при малой яркости.

В). Основные правила использования логических ударений

Для оптимизации изучения информации на экране компьютера при разработке презентаций рекомендуется использование логических ударений. *Логическими ударениями принято называть психолого-аппаратные приемы, направленные на привлечение внимания пользователя к определенному объекту*. Психологическое действие логических ударений связано с уменьшением времени зрительного поиска и фиксации оси зрения по центру главного объекта.

Наиболее часто используемыми приемами для создания логических ударений являются: *изображение главного объекта более ярким цветом; изменение размера, яркости, расположения; выделение проблесковым свечением.*

Правило 1. Количественной оценкой логического ударения является его интенсивность. Интенсивность зависит от соотношения цвета и яркости объекта по отношению к фону, от изменения отно-

сительных размеров объекта по отношению к размерам предметов фона изображения.

Правило 2. Наиболее предпочтительным является выделение либо более ярким, либо более контрастным цветом, менее предпочтительно выделение проблесковым свечением, изменением размера или яркости.

Правило 3. В случае использования режима мигания объекта в компонентах презентации рекомендуется фиксировать частоту мигания в пределах 3-8 Гц (миганий в секунду).

Правило 4. Для привлечения внимания к объекту слайда презентации возможно использование нескольких логических ударений одновременно. Тогда интенсивность логического ударения объекта будет равна сумме этих логических ударений. Например, объект может быть выделен одновременно уменьшением яркости фона, включением режима его мигания или проблескового свечения и звуковыми сигналами.

Правило 5. Одновременное выделение в отдельных слайдах или целом по всей презентации нескольких объектов логическими ударениями с близкой интенсивностью приводит к рассеиванию внимания и, как следствие, к быстрому развитию утомления.

Правило 6. На эстетико-эргономические показатели презентации и комфортность восприятия зрительной информации существенное влияние оказывает степень засоренности поля главного объекта. Рекомендуется размещать в поле главного объекта не более 4-6 второстепенных объектов. Увеличение числа второстепенных объектов может привести к рассеиванию внимания и, как следствие, к выпадению главного объекта из области внимания, либо к слиянию второстепенных объектов с фоном.

Правило 7. Формы объектов и элементов фона изображения должны соответствовать устойчивым зрительным ассоциациям, должны быть похожи на формы реальных предметов, объектов. Несоответствие этому требованию может привести к ненужным вопросам и, как следствие, к потере времени представления презентации.