Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра компьютерной безопасности и математического обеспечения
информационных систем

Ю.Д. Фот

ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические указания

Рекомендовано к изданию редакционно-издательским советом федерального государственного бюджетного образовательного учреждения высшего образования «Оренбургский государственный университет» для обучающихся по образовательной программе высшего образования по специальности 10.05.01 Компьютерная безопасность

Оренбург
2019

УДК 34(076.5)
ББК 67я7
Ф 81

Рецензент – кандидат технических наук Ю.В. Полищук

Фот, Ю.Д.

Ф 81 Организационное и правовое обеспечение информационной безопасности : методические указания / Ю.Д. Фот; Оренбургский гос. ун-т. – Оренбург : ОГУ, 2019. – 57с.

Методические указания по дисциплине «Организационное и правовое обеспечение информационной безопасности» содержат рекомендации к практическим занятиям.

Методические указания разработаны на основании учебного плана ФГБОУ ВО ОГУ и предназначены для студентов очной формы обучения по специальности 10.05.01 Компьютерная безопасность, имеющих специализацию «Разработка защищенного программного обеспечения».

УДК 34(076.5)
ББК 67я7

Содержание

Введение

Практические занятия - одна из форм аудиторных занятий, на которых студенты под руководством преподавателя приобретают необходимые умения и навыки по тому или иному разделу определенной дисциплины, входящей в учебный план.

Цель практических занятий по дисциплине «Организационное и правовое обеспечение информационной безопасности» - предоставление возможностей для углубленного изучения теории и нормативно-правовой базы в области организационной и правовой защиты информации, овладения практическими навыками и выработки самостоятельного творческого мышления у студентов.

Задачи практических занятий по дисциплине «Организационное и правовое обеспечение информационной безопасности»:

– углубление теоретической и практической подготовки студентов по знаниям основных нормативно-правовых документов, регламентирующих организационную безопасность;

– приближение учебного процесса к реальным условиям работы специалиста в области информационной безопасности;

– формирование умения применять полученные знания на практике, осуществлять анализ безопасности компьютерных систем на соответствие отечественным и зарубежным нормативно-правовым документам и стандартам в области компьютерной безопасности;

– проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем на основе нормативно-правовой базы регуляторов;

– способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия при анализе безопасности компьютерных систем на соответствие отечественным и зарубежным нормативно-правовым документам и стандартам в области компьютерной безопасности;

– использовать основы экономических знаний при расчете ущерба информационной безопасности компьютерным системам на основе нормативно-правовой базы, определять рациональные меры по обеспечению организационной и правовой защиты;

– формирование навыков публичного выступления, способности представлять результаты проведенного исследования, умения вести дискуссию;

– формирование общих и профессиональных компетенций;

– контроль за освоением учебной дисциплины.

Для достижения поставленных целей и решения требуемого перечня задач, практические занятия по дисциплине проводятся с использованием новых образовательных технологий.

Практические занятия по дисциплине «Организационное и правовое обеспечение информационной безопасности» проводятся в следующем виде:

– контрольно-обучающий семинар - занятие, в ходе которого осуществляется фронтальный опрос;

– обучающий семинар - это занятие, на котором в центре внимания самостоятельные выступления студентов;

– творческая дискуссия, диспут, публичная защита рефератов;

– практическое занятие по анализу ситуаций и выполнения расчетно-графического задания.

1 Практическое занятие № 1. Нормативно-методическая база в области национальной безопасности РФ. Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации.

Форма проведения практического занятия:

– первая часть занятия проводится в виде опроса и рассмотрения задач (ситуаций).

– вторая часть занятия проводится в виде выполнения РГЗ.

Цель занятия:

Изучить нормативно-методическую базу в области национальной безопасности РФ и научиться выявлять объекты государственной и негосударственной собственности, которые относятся к КВО для национальной безопасности РФ

Вопросы для опроса:

1. Место информационной безопасности в общей системе безопасности РФ.
2. Основные задачи государственной системы защиты информации.
3. Организационная структура государственной системы защиты информации.
4. Функциональная структура государственной системы защиты информации.
5. Что такое Доктрина ИБ РФ?
6. Перечислите основные составляющие национальных интересов РФ в информационной сфере.
7. Дайте определение ИБ.

8. Сформулируйте интересы государства, общества и личности в информационной сфере.

9. Сформулируйте основные направления международного сотрудничества Российской Федерации в области ИБ.

10. Перечислите основные функции системы обеспечения ИБ.

11. Как подразделяются общие методы обеспечения ИБ?

12. Каковы особенности обеспечения ИБ РФ в сферах экономики, внешней политики, внутренней политики, областях науки и техники, сфере духовной жизни, информационных и телекоммуникационных системах, в сфере обороны, правоохранительной и судебной сферах, в условиях чрезвычайных ситуаций?

13. В чем заключаются национальные интересы и безопасность РФ.

14. Сформулируйте определение безопасности в соответствии с Федеральным законом № 390 «О безопасности».

15. Назовите основные принципы обеспечения безопасности.

16. Какие риски и угрозы несет несоблюдение экономической, политической, социальной, экологической, военной, культурной, информационной безопасностей?

17. В каком документе отражена задача укрепления информационной безопасности?

18. Какие сложности возникают при решении задачи по обеспечению защиты граждан и государства в информационной сфере?

19. Какие задачи информационной безопасности должны быть решены на период до 2020 года?

20. Какие существуют методы обеспечения информационной безопасности в соответствии с Доктриной информационной безопасности? Что они в себя включают?

21. Дайте определение терминам «информационные технологии», «обладатель информации», «доступ к информации», «документированная информация», «защита информации», «защита информации от утечки», «защита информации от преднамеренного воздействия», «защита информации от НСД», «техническая защита конфиденциальной информации», «система защиты информации», «средство

защиты информации», «средство контроля эффективности защиты информации», «объект информатизации», «защищаемый объект информатизации», «основные технические средства и системы», «вспомогательные технические средства и системы», «защищаемые помещения», «лицензирование», «сертификация», «аттестация объектов информатизации», «неотказуемость», «подотчетность», «аутентичность», «достоверность».

22. Правовая защита – направление защиты информации. Государственное регулирование информационной безопасности. Доктрина информационной безопасности РФ.

23. Организационная защита – направление защиты информации. Содержание основных организационных мероприятий. Функционал службы защиты информации.

24. Инженерно-техническая защита – направление защиты информации. Классификация средств инженерно-технической защиты. Краткая характеристика основных классов.

РГЗ - Ознакомление с Методикой отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации

Цель РГЗ: Изучить методику отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации. Спроектировать информационную систему и описать потенциально опасные объекты, относящиеся к государственной и негосударственной собственности.

Для выполнения РГЗ необходимо выбрать объект для исследования. Объект выбирается учащимся самостоятельно, либо выдаётся преподавателем.

Объект необходимо отнести к одной или нескольким из следующих групп:

1. Субъекты природных монополий, которые ведут деятельность на общегосударственном рынке товара;

2. Организации, занимающие монопольное (доминирующее) положение на общегосударственном рынке товаров при условии, что этот товар имеет важное социально-экономическое значение;

3. Организации топливно-энергетического комплекса, которые входят в объединенную энергетическую систему;

4. Организации оборонно-промышленного комплекса, составляющие научно-технический потенциал страны; имеющие значительный удельный вес в объеме стоимости экспорта товаров, работ, услуг;

5. Организации, на которых работают более 10 тыс. человек;

6. Организации, которые входят в категорию крупных налогоплательщиков;

7. Организации, обеспечивающие функционирование инфраструктуры общегосударственного значения, в частности информационно-телекоммуникационные, электросвязи и почты, железнодорожного, авиационного и морского транспорта, магистральных газо- и нефтепроводов, инженерные сооружения (мосты, тоннели);

8. Организации, добывающие и перерабатывающие полезные ископаемые общегосударственного значения.

9. Объекты информационной и телекоммуникационной инфраструктуры.

10. Объекты культурного наследия.

* если объект не удалось отнести ни к одной из групп, данный объект не относится к КВО.

Ход выполнения работы:

1. Скачайте программу «Автоматизированная система отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации» https://ufer.osu.ru/index.php?option=com_uferdbsearch&view=uferdbsearch&action=details&ufer_id=1660.

2. Откройте программу «Методика отнесения к КВО_64bit.exe», в главном окне введите количество объектов, существующих в вашей информационной системе:

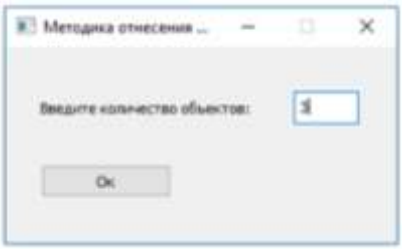

Рисунок 1.1 – Введение количества анализируемых объектов

Примечание: обратите внимание, что в поле должно быть введено положительное число – количество объектов. В противном случае будет получена ошибка:

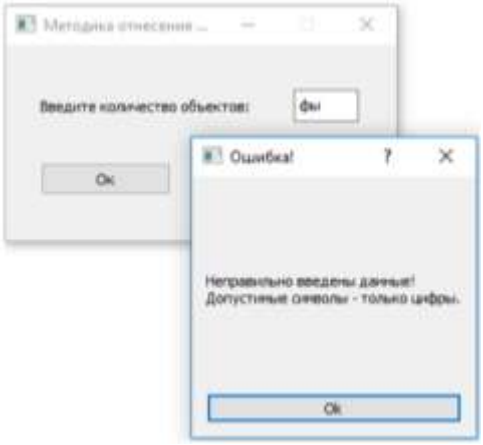

Рисунок 1.2 – Информация об ошибке

Далее нажмите кнопку «ок», откроется следующее окно с основными критериями оценки. В белые ячейки необходимо ввести положительные значения (действительные числа, пример: 4, 4.15 и т.д.). Первоначальная оценка производится по 6 критериям:

П1 – стоимость годового выпуска товарной продукции;

П2 – общая численность производственного персонала;

П3 – балансовая стоимость основных производственных фондов;

П4 – доля основной продукции объекта в продукции того же вида, выпускаемой в стране;

П11 – территория заражения (загрязнения) в случае аварии на объекте;

П12 – численность населения, которое может пострадать в случае аварии на объекте.

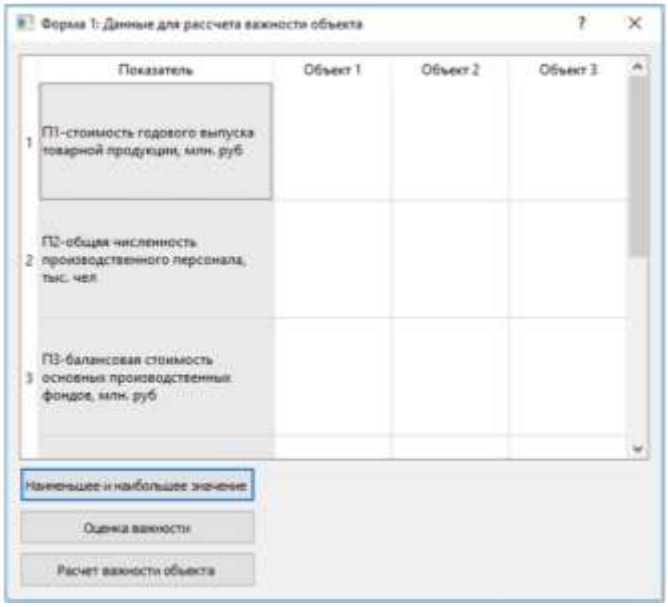

Рисунок 1.3 – Данные для расчета важности объекта

Примечание: если хотя бы одно поле останется пустым или будет заполнено нечисловым значением, программа выдаст ошибку:

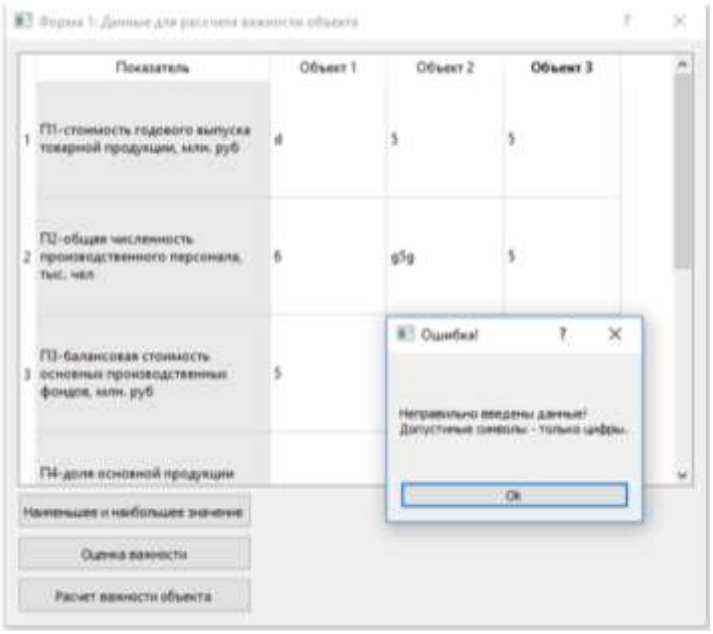

Рисунок 1.4 – Сведения об ошибке

После того, как заполнены все значения можно вычислить минимум и максимум для объектов по каждому из критерий, для этого достаточно начать кнопку «Наименьшее и наибольшее значение»:

Рисунок 1.5 – Представление наименьших и наибольших значений

Закроем окно с наименьшими и наибольшими значениями. Откроем окно с оценкой важности объекта, кликов на кнопку «Оценка важности». Для введенных объектов откроется следующее окно:

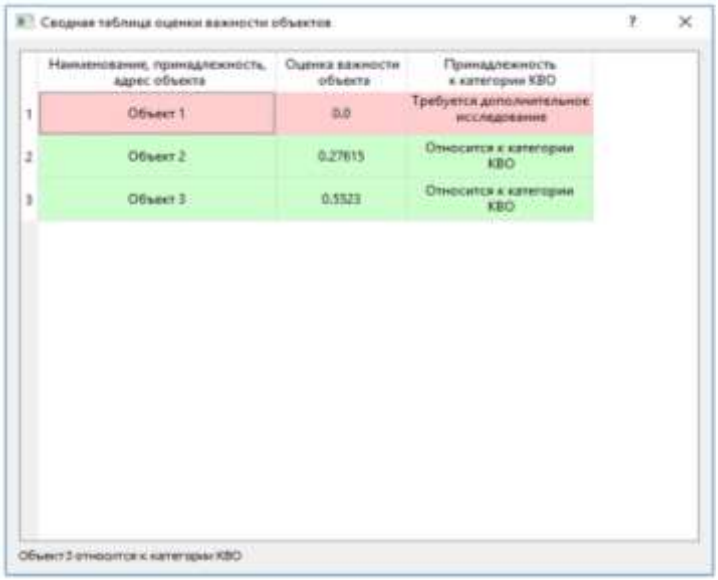

Рисунок 1.6 – Сводная таблица оценки важности объектов

Красный цвет указывает на то, что объект не относится к критически важным. Зеленым цветом отмечены объекты, которые относятся к критически важным объектам.

По каждому из введенных показателей для каждого объекта вычисляется его вклад в оценку важности по формуле:

$$Y_i = k_i \frac{(X_i - m)}{(M - m)} \quad , \tag{1.1}$$

где м и М – соответственно минимальное и максимальное значения показателя множества рассчитываемых объектов;

X – фактическое значение показателя для рассматриваемого объекта;

k – коэффициент значимости рассматриваемого показателя.

Если значение получается больше 0.25 значит, объект относится, к критически важным, в противном случае – не относится и требует дополнительных исследований.

Из примера видно, что объект 1 требует дополнительных исследований. Проведем их, закрыв окно и в главном окне нажав кнопку «Расчет важности объектов». Откроется окно выбора объекта для уточнения:

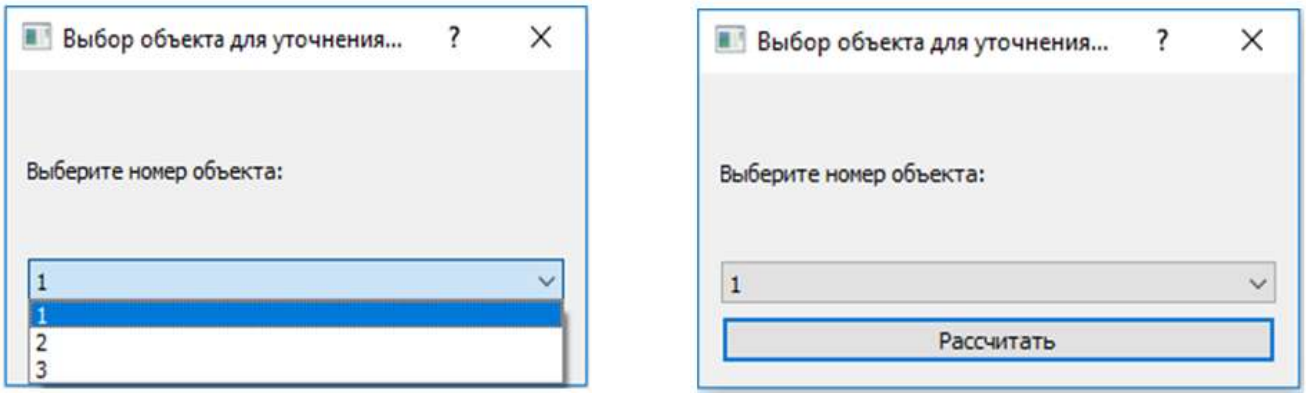

Рисунок 1.7 – Выбор объекта уточнения

Из раскрывающегося списка выберем нужный объект и нажмем кнопку «рассчитать»:

Откроется окно с полным списком критериев:

Рисунок 1.8– Расчет важности объекта

В белые ячейки необходимо ввести значение «0» если критерий не важен и «1», если критерий для объекта важен. Таким образом заполнить все пустые ячейки в колонке «фактическое значение на объекте Х».

Примечание: если в ячейке вводится значение отличное от «1» и «0» будет получена ошибка:

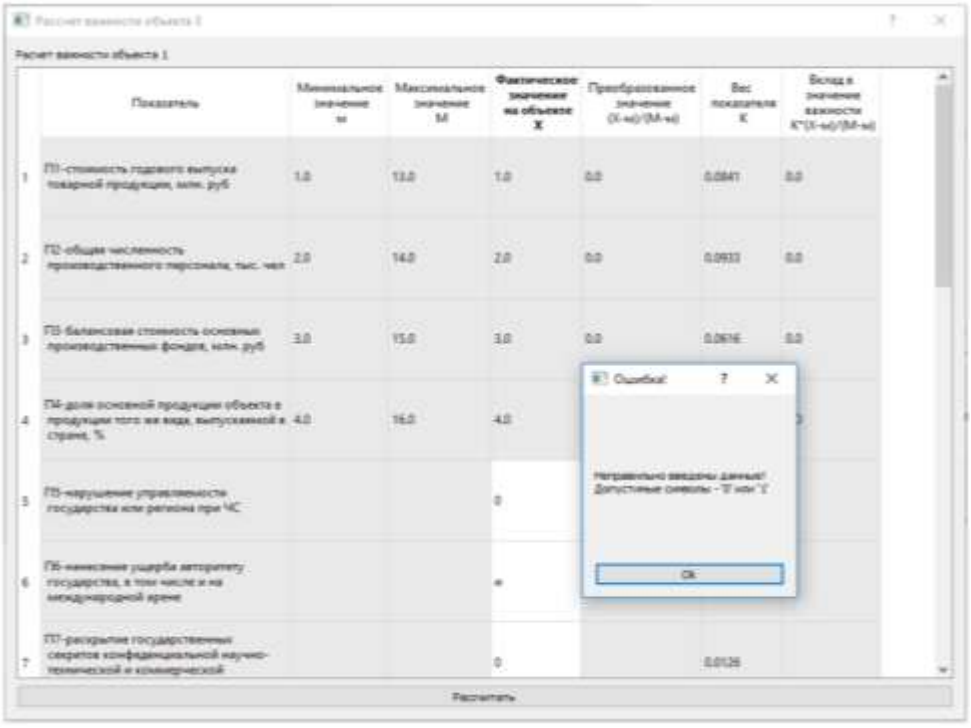

Рисунок 1.9 – Ошибка при расчете важности объекта

После заполнения таблицы необходимо нажать на кнопку «рассчитать», вклад в значение важности будет рассчитан автоматически и клетка со значением будет подсвечена зеленым – если объект стал критически важным, и красным в противном случае.

3. Значение показателя важности рассматриваемого объекта определяется, как сумма вкладов в значение важности каждого из показателей.

Проанализируйте полученные результаты. Сделайте выводы по проведенной работе в отношении разработанной информационной системы.

Список источников для самоподготовки

1. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации»;
2. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
4. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;
5. Федеральный закон от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Российской Федерации»;
6. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»;
7. Основами государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 № Пр-1753);
8. Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации (утв. МЧС России 17.10.2012 № 2-4-87-23-14).

2 Практическое занятие № 2. Структура органов власти по защите информации. Понятия и виды защищаемой информации

Форма проведения практического занятия:

– первая часть занятия проводится в виде опроса и рассмотрения структуры органов власти по защите информации.

– вторая часть занятия проводится в виде выполнения РГЗ.

Цель занятия:

Изучить структуру органов власти по защите информации, взаимодействие органов обеспечения информационной безопасности, функции каждого из участников этого процесса.

Вопросы для опроса:

1. К каким последствиям может привести утрата конфиденциальной информации.
2. От кого Вы защищаете конфиденциальную информацию.
3. Что называется коммерческой тайной?
4. Что такое служебная тайна?
5. Что представляет профессиональная тайна?
6. Что такое информация ограниченного распространения?
7. Каковы виды доступа к информации?
8. Что такое персональные данные?
9. Что такое конфиденциальная информация, государственная и коммерческая тайна?
10. Назовите три категории ценности коммерческой информации.
11. Что такое товарная ценность информации и каковы пути ее получения?
12. На основе, каких документов проводится анализ информационных активов предприятия?

13. Какие виды информации ограниченного доступа Вы знаете? Перечислите их.

14. Обсуждение структуры органов власти по защите информации, представленной на рисунке

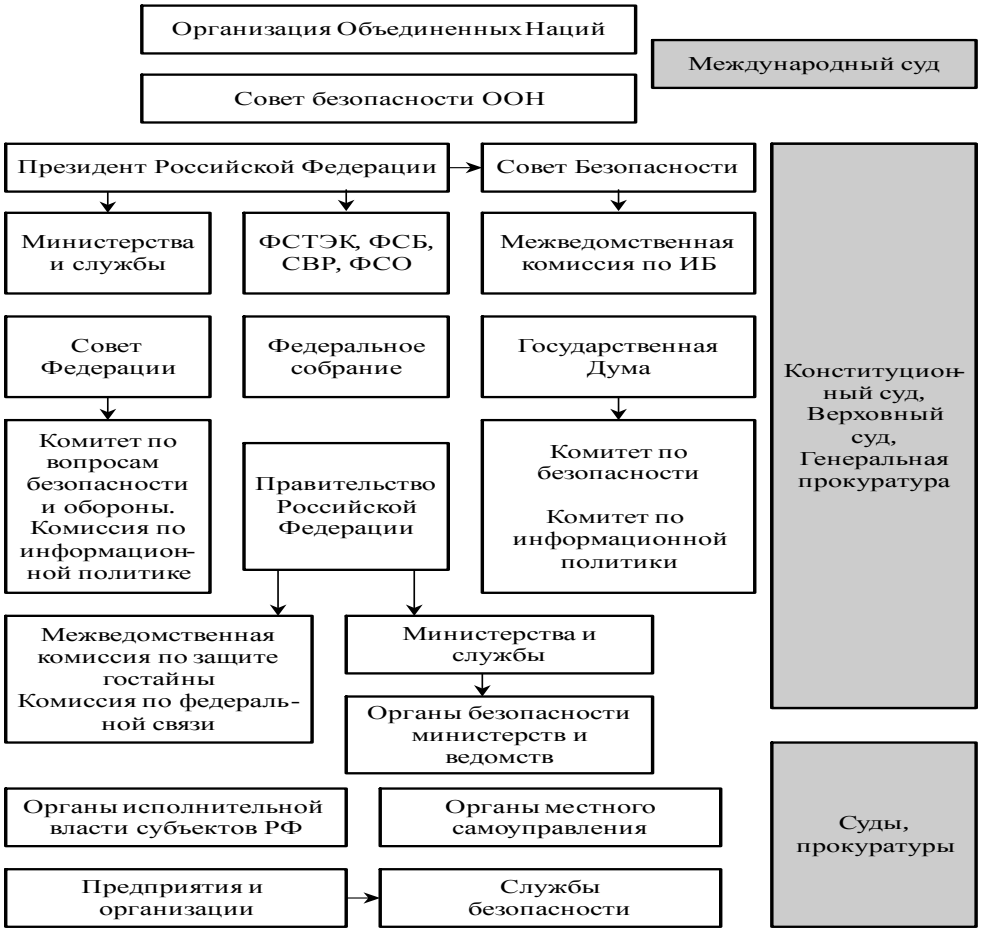

Рисунок 2.1- Структура органов власти по защите информации

15. Что такое Коммерческая тайна? Что нельзя отнести к коммерческой тайне?

16. Что такое служебная информация? Какие виды информации Вы можете отнести к служебной тайне?

17. Что такое профессиональная тайна? Какие виды информации Вы можете отнести к профессиональной тайне?

18. Что такое интеллектуальная собственность? Какие виды информации Вы можете отнести к интеллектуальной собственности?

19. Что такое активы предприятия? Что такое информационные активы? Как правильно их проанализировать?

20. Понятие и виды информации, защищаемой законодательством Российской Федерации. Основные концептуальные положения системы защиты информации.

21. Правовое регулирование технологического обмена. Защита интеллектуальной собственности. Критерии ценности документов.

22. Предпосылки к разглашению сведений, составляющих коммерческую тайну. Экспертиза ценности документов.

23. Назовите основные мероприятиями по защите от разглашения конфиденциальной информации.

РГЗ - Понятия и виды защищаемой информации

Цель РГЗ: Научиться выявлять виды информации ограниченного доступа на предприятии и относить к одной из групп конфиденциальности либо секретности.

Студент выбирает любое предприятие, информационную систему которого будет исследовать в работе.

Информация может храниться в различных формах, включая такие как цифровая форма (например, файлы с данными, сохраненные на электронных или оптических носителях), материальная форма (например, на бумаге), а также в нематериальном виде в форме знаний служащих. Информация ограниченного доступа на предприятии отражена в активах предприятия. *Актив* – это что-либо, что имеет ценность для организации[1]. В соответствии с ГОСТ Р ИСО/МЭК 27000-2012, имеются различные типы активов, представленные на рисунке.

Рисунок 2.2 – Типы активов

[1]ГОСТ Р ИСО/МЭК 27000-2012 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (утв. и введен в действие Приказом Росстандарта от 15.11.2012 N 813-ст)

Информационный актив (information asset) - знания или данные, которые имеют значение для организации[2].

Ход выполнения работы:

1. Проанализировать информационные активы выбранного вами предприятия: Укажите месторасположение информационных активов по отделам

Таблица 2.1– Анализ информационных активов

Информационный актив (S)	Характеристики информационных активов			
	Место хранения	Вид хранения	Срок хранения	Обоснование нормативно-правовой базы
s_1	…		…	…
s_2	…	…	…	
…	…	…	…	…
s_i		…	…	…

2.Перечень информационных активов при построении системы защиты информации можно представить в виде отношения сведений $S=\{s_i\}$ и уровня их конфиденциальности $A=\{a_k\}$, где i – номер оцениваемого сведения, а k – упорядоченное множество значений лингвистической переменной «категория закрытой информации» = {<Открытая, несекретная информация (ОИ)>, <Персональные данные (ПДн)>, <Коммерческая тайна (КТ)>, <Служебная тайна (СТ)>, <Секретно (С)>, <Совершенно секретно (СС)>, <Особой важности (ОВ)>, <Для служебного пользования (ДСП)>, ….}.

Таблица 2.2 – Условное представление перечня информационных активов

Информационный актив (S)	Уровни конфиденциальности (A)			
	a()	a_1	…	a_k
s_1	…	s_1a_1	…	…
s_2	…	…	…	S_2a_k
…	…	…	…	…
s_i	$s_ia_{()}$	…	…	…

[2]ГОСТ Р ИСО/МЭК 27000-2012 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (утв. и введен в действие Приказом Росстандарта от 15.11.2012 N 813-ст)

3. Отразите взаимосвязи между информационными активами и критериями их безопасности.

Таблица 2.3 - Отражение взаимосвязи между информационными активами и критериями их безопасности

Информационный актив (S)	Критерии безопасного состояния информационного актива					
	Конфиденциальность (e_1)	Целостность (e_2)	Доступность (e_3)	Подотчетность (e_4)	Аутентичность (e_5)	Достоверность (e_6)
s_1	$s_1a_2e_1$	…	s_1e_3	…	…	…
s_2	$s_2a_2e_1$	…	…	…	…	…
…	…	…	s_ie_3	…	…	…
s_i	$s_ia_2e_1$	…	…	…	…	…

Атрибуты $s_ia_ke_j$ будут означать, что информация ограниченного доступа s_i имеет уровень конфиденциальности a_k и относится к категории безопасного состояния e_j.

4. Изучите технологический процесс обработки и хранения информации, физических условий и условий окружающей среды на выбранном предприятии:

– внешние подключения с другими системами – протоколы взаимодействия;

– хранение информации – файловая организация и архивация;

– накопление информации – каналы, носители, накопители, обмен информации, фактографическая информация, репликация, архивация, обновления, предоставление информации разным категориям пользователей;

– способ предоставления информации – сайты, почта и вывод на печать, мобильные пользователи, требования в работе с документированной информацией

– средства обработки и передачи информации, технические и программные средства ВТ, средства и линии связи, предоставляющие возможности как для перемещения (передачи, копирования) информации между различными областями памяти и информационными носителями, различными средствами обработки, определенными для АС, так и по выводу информации из установленной для нее сферы обращения.

Список источников для самоподготовки

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

2. Федеральный закон от 21.07.1993 № 5485-1 «О государственной тайне»;

3. Указ Президента РФ от 30.11.1995 № 1203 (ред. от 05.10.2017) «Об утверждении Перечня сведений, отнесенных к государственной тайне»;

4. Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера».

3 Практическое занятие № 3. Режим защиты государственной тайны

Форма проведения практического занятия:

– первая часть занятия проводится в виде опроса и рассмотрением задач (ситуаций).

– вторая часть занятия проводится в виде выполнения и защиты реферата.

Цель занятия:

Изучить информационное законодательство, юридические механизмы обеспечения информационной безопасности сведений, составляющих государственную тайну. Научиться работать с нормативными актами, применять их в практической деятельности; применять правовые механизмы обеспечения информационной безопасности сведений, составляющих государственную тайну.

Вопросы для опроса:

1. Что такое государственная тайна?
2. Назовите три степени секретности.
3. Понятие государственной тайны.
4. Полномочия органов государственной власти в области защиты государственной тайны.
5. Порядок отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
6. Допуск к государственной тайне.
7. Защита государственной тайны.
8. Концептуальные основы защиты государственной тайны.
9. Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.

10. Реквизиты носителей сведений, составляющих государственную тайну.

11. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания.

12. Основные классы документов по защите государственной тайны: правовые; организационно-распорядительные; нормативные; плановые; информационные.

13. Органы государственной власти, предприятия, учреждения, организации и их структурные подразделения по защите государственной тайны

14. Порядок допуска должностных лиц и граждан к государственной тайне.

15. Особенности допуска лиц, имеющих двойное гражданство, лиц без гражданства, а также лиц из числа иностранных граждан, эмигрантов и реэмигрантов, к государственной тайне.

16. Особый порядок допуска к государственной тайне.

17. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне.

18. Организация защиты информации, составляющей государственную тайну, на предприятиях, в организациях и учреждениях.

19. Особенности защиты информации в условиях реализации международных договоров по сокращению вооружений и вооруженных сил.

20. Особенности защиты информации в условиях создания совместных предприятий.

21. Особенности защиты информации в условиях научно-технического, военно-технического и экономического сотрудничества с другими странами.

Темы рефератов:

1. Конституция Российской Федерации о защите государственной тайны.
2. Концепция защиты государственной тайны в Российской Федерации.
3. Закон Российской Федерации «О безопасности» как правовая основа защиты государственной тайны.
4. Полномочия Президента РФ в сфере защиты государственной тайны.

5. Особенности защиты государственной тайны в условиях научно-технического, военно-технического и экономического сотрудничества с другими странами.

6. Порядок допуска должностных лиц и граждан РФ к государственной тайне.

7. Особенности допуска к государственной тайне лиц, имеющих двойное гражданство, апатридов, иностранных граждан, эмигрантов и реэмигрантов.

8. Технические средства защиты информации и их применение в области защиты государственной тайны.

9. Государственная политика информационной безопасности и организационная основа ее обеспечения.

10. Особенности защиты государственной тайны в условиях реализации международных договоров по сокращению вооружений и вооруженных сил.

11. Особенности защиты государственной тайны в условиях создания совместных предприятий.

Список источников для самоподготовки

1. Федеральный закон от 21 июля 1993 г. № 5485-I «О государственной тайне»;

2. Постановление правительства РФ от 18 сентября 2006 г. № 573 г. О предоставлении социальных гарантий гражданам, допущенным к государственной тайне на постоянной основе, и сотрудникам структурных подразделений по защите государственной тайны;

3. Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».

4 Практическое занятие № 4. Защита персональных данных

Форма проведения практического занятия:

– первая часть занятия проводится в виде опроса и рассмотрением задач (ситуаций).

– вторая часть занятия проводится в виде выполнения РГЗ.

Цель занятия:

Изучить нормативно-методическую базу в области защиты ИСПДн, изучить методику определения уровня защищенности ИСПДн.

Вопросы для опроса:

1. Что такое Персональные данные? Какие категории ПДн Вы знаете?
2. Нормативно-правовое обеспечение защиты персональных данных
3. Система государственного контроля и надзора за обеспечением безопасности персональных данных
4. Обязанности и ответственность операторов персональных данных
5. Угрозы информационным системам персональных данных
6. Описание информационных систем персональных данных
7. Классификация информационных систем персональных данных
8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах
9. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах
10. Организация защиты информационных систем персональных данных и реализация системы защиты персональных данных
11. Мероприятия по защите персональных данных при их обработке в информационных системах

12. Порядок применения криптографических средств для защиты персональных данных

13. Оптимизация системы защиты персональных данных

14. Организационные и технические меры безопасности при хранение персональных данных на носителях

15. Документальное обеспечение деятельности оператора персональных данных

16. Алгоритм действий оператора по приведению ИСПДн в соответствие законодательству.

17. Кто может проверить оператора? Что, как и когда может проверять Роскомнадзор? Что, как и когда может проверять ФСТЭК?

18. Какова процедура проверки со стороны РКН?

19. Примерный перечень документов, отрабатываемых при приведении ИСПДн в соответствие законодательству.

20. Особенности обеспечения безопасности информации при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных.

21. Особенности обеспечения безопасности информации при ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях.

22. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

23. Состав мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах (в соответствии с ППРФ № 1119)

24. Основные положения методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации

РГЗ - Методика определения актуальных угроз в ИСПДн. Требования к системе защиты ИСПДн

Цель РГЗ: Научиться строить частную модель угроз и нарушителя в соответствии с базовой моделью угроз и методикой определения актуальных угроз ИСПДн, научиться определять уровень защищенности ИСПДн и формировать требования по их защите в соответствии с нормативно-методической базой ФСТЭК и ФСБ.

Для выполнения РГЗ необходимо выбрать объект для исследования. Объект выбирается учащимся самостоятельно, либо выдаётся преподавателем.

Объектом исследования должна быть информационная система обработки персональных данных государственной организации. Например: ИСПДн налогоплательщиков, ИСПДн министерства, ИСПДн сотрудников любого государственного учреждения и т.д.

Ход выполнения работы:

1. Проведите анализ организации безопасности ПДн в выбранной Вами ИСПДн:

- каким образом происходит обработка ПНд;
- цель обработки ПДн;
- правовое основание обработки ПДн;
- перечень обрабатываемых ПДн и объем ПДн, перечень осуществляемых действий в отношении ПДн в ИСПДн;
- сроки хранения ПДн;
- способы поступления и ввода ПДн в ИСПДн;
- источники поступления ПДн;
- информация об организации передачи ПДн.

Пример таблиц для анализа организации безопасности ПДн

Таблица 4.1 – Способ обработки ПДн

ИСПДн	Способ обработки	Описание процесса обработки
«Кадровый учет»	Автоматизированная	Сотрудник составляет трудовые договоры

Таблица 4.2 –Цель обработки ПДн

ИСПДн	Цель
«Кадровый учет»	Ведение кадрового учета

Таблица 4.3 – Правовое обоснование обработки ПДн

ИСПДн	Правовое основание обработки ПДн
«Кадровый учет»	Трудовой кодекс РФ

Таблица 4.4 – Категория и объем ПДн

ИСПДн	Обрабатываемые ПДн	Категория ПДн	Объем ПДн
«Кадровый учет»	Фамилия, имя, отчество, паспортные данные, ИНН, СНИЛС, должность, данные об образовании, телефон, квалификация.	Категория 2: Данные, позволяющие идентифицировать субъекта и получить о нем дополнительную информацию	

Таблица 4.5 -Перечень осуществляемых действий в отношении ПДн в ИСПДн

ИСПДн	Действия
«Кадровый учет»	Сбор, систематизация, накопление, хранение, уточнение (изменение, обновление), использование, уничтожение, передача.

Таблица 4.6– Сроки хранения

ИСПДн	Срок хранения
«Кадровый учет»	75 лет

Таблица 4.7– Ввод Пдн

ИСПДн	Ввод ПДн
«Кадровый учет»	С клавиатуры

Таблица 4.8– Источники поступления ПДн

ИСПДн	Источники поступления ПДн
«Кадровый учет»	От сотрудников организации

Таблица 4.9– Передача ПДн

ИСПДн	Передача ПДн	Объем предоставляемых ПДн
«Кадровый учет»	Передаются в обслуживающий организацию банк, налоговую службу, пенсионный фонд.	Вся БД

2. Откройте Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Определите какую категорию ПДн обрабатывает ваша система.

3. Проведите анализ автоматизированной системы обработки ПДн в выбранной Вами ИСПДн: ЛВС, Сетевое оборудование, программное и техническое обеспечение каждой ИСПДн, схема структуры сети, обеспечение безопасности работы в сети Интернет.

Таблица 4.10 - Анализ автоматизированной системы обработки ПДн

ИСПДн	Конфигурация, логическая структура	Состав ТС	Наличие физических подключений (ЛВС, Интернет, каналы связи провайдеров)
«Кадровый учет»	Специальная автономная многопользовательская без разграничения прав доступа	7 АРМ	ИСПДн не подключена к сетям общего пользования

Таблица 4.11 - Анализ автоматизированной системы обработки ПДн

Наименование, версия ОС	Месторасположение	Примечание
Microsoft Windows XP Professional SP 3	г. Оренбург, ул. М. Горького, д. 28, отдел кадров, приемная	АРМ. Сертификат ФСТЭК не предоставлен
Наименование, версия	Возможности программного средства	Расположение ресурса
ИСПДн «Кадровый учет»		
Microsoft Office, для дома и бизнеса 2010	Текстовый редактор	Отдел кадров Системный блок Инв.№ 013660053

4. Откройте нормативно-методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» ФСТЭК России, 2008 год. На его основе проведите анализ источников угроз ИСПДн.

Источниками угроз НСД в ИСПДн могут быть: нарушитель; носитель вредоносной программы; аппаратная закладка.

Таблица 4.12 - Характеристика различных типов нарушителей ИСПДн

Тип	Угрозы	Причины (цели)	Квалификация, потенциал	Используемые методы и средства
Внутренний нарушитель	Несанкционированное использование ПДн; Модификация документов, обрабатываемых ПДн; Передача третьим лицам.	Получение личной выгоды; Личные просьбы друзей, знакомых; Безответственность; Саботаж; Месть; Неудовлетворенное тщеславие.	Работает с ПДн, имеет доступ к ним. Может скрыть неправомерную деятельность.	Использует недостатки используемых информационных технологий, ошибки пользователей и администраторов.

5. На основе нормативно-методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» ФСТЭК России, 2008 год. проведите классификацию уязвимостей ИСПДн.

Таблица 4.13 - Анализ уязвимостей ИСПДн

Наименование (характеристика) уязвимости	Содержание нарушения безопасности информации
1. Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде) 2. Доступ по умолчанию 3. Наличие двух открытых портов	Возможность перехвата данных учетной записи (имен зарегистрированных пользователей, паролей). Получение удаленного доступа к хостам

6. Откройте нормативно-методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России, 2008 год. На его основе вычислите уровень исходной защищенности ИСПДн (Y_1).

7. Составьте перечень угроз, учитывая источники угроз и уязвимости. При составлении угроз используйте Банк данных угроз информационной безопасности ФСТЭК https://bdu.fstec.ru/.

Используя нормативно-методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК России:

- определите частоту (вероятность) реализации угрозы (Y_2). Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

- рассчитайте вероятность реализации угрозы (Y), определите опасность угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y=(Y1 +Y2)/20$.

- оцените опасность каждой угрозы (О). При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн.

- определите актуальность угрозы для данной ИСПДн.

Заполните таблицу.

Таблица 4.14 - Анализ актуальности угроз ИСПДн

Угроза	Реализованные контрмеры	Y_2	Y	О	Актуальность угрозы
Угроза наличия недокументированных (недекларированных) возможностей в системном ПО, используемом в ИС	Обрабатываемые в ИСПДн персональные данные не представляют интереса для лиц, имеющих возможность внедрения программных закладок на этапах разработки, поставки и обновления системного ПО ИСПДн.	Мал. (0)	0,5 (Ср.)	Низ.	Неакт.

8. Откройте Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». На его основе

определите к какому типу угроз относятся выявленные актуальные угрозы ИСПДн и к какому уровню защищенности относится ваша ИСПДн.

9. Откройте Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». Определите состав организационных и технических мер по обеспечению безопасности в соответствии с уровнем защищенности вашей ИСПДн.

10. Осуществите выбор средств защиты информации для ИСПДн, используя Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00). Для более точного определения класса средств защиты информации используйте данные, представленные в таблице.

Таблица 4.15 - Выбор средств защиты информации для ИСПДн

СЗИ сертифицированные по Требованиям безопасности	Уровни защищенности ИСПДн				
	IV уровень защищенности	III уровень защищенности		I и II уровень защищенности	
		Без Internet	С Internet	Без Internet	С Internet
1	2	3	4	5	6
Классы средств вычислительной техники (СВТ)	6 класс	5 класс	5 класс	5 класс	5 класс
Классы систем обнаружения вторжений (СОВ)	5 класс	5 класс (актуальны угрозы 3-го типа)	4 класс (актуальны угрозы 2-го типа)	4 класс	4 класс
Классы средств антивирусной защиты (САВЗ)					

Продолжение таблицы 4.15

1	2	3	4	5	6
Классы межсетевых экранов (МЭ)	5 класс	4 класс (актуальны угрозы 3-го типа)	3 класс (актуальны угрозы 2-го типа)	4 (актуальны угрозы 3-го типа)	3 (или актуальны угрозы 1-го, 2-го типов)
Уровни контроля отсутствия недекларированных возможностей (НДВ)		4 класс (актуальны угрозы 2-го типа)		4 класс	4 класс

11.Если персональные данные в вашей ИСПДн подлежат криптографической защите в соответствии с законодательством Российской Федерации или в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью средств криптографической защиты информации, то откройте «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности № 149/7/2/6-432 от 31 марта 2015 года». Дополните разработанную Вами частную модель угроз дополнительным анализом.

Таблица 4.16 - Анализ возможности источников атак ИСПДн

Обобщенные возможности источников атак	Да/Нет
Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	
….	…

Таблица 4.17 - Уточнѐнные возможности нарушителей и направления атак ИСПДн

Уточнѐнные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
…	…	…

Более подробные рекомендации по заполнению таблиц, представлены в методических рекомендациях.

12. Если персональные данные в вашей ИСПДн подлежат криптографической защите в соответствии с законодательством Российской Федерации или в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью средств криптографической защиты информации, то определении состава организационных и технических мер защиты информации Вашей ИСПДн используйте Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

13. Осуществите выбор средств криптографической защиты информации для ИСПДн, используя Перечень средств защиты информации, сертифицированных ФСБ России (http://clsz.fsb.ru/certification.htm).

Список источников для самоподготовки

1. Руководящий документ ФСТЭК России 15.02.2008 г. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

2. Руководящий документ ФСТЭК России 14.02.2008 г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

3. Руководящий документ ФСБ РФ 31.03.2015 г. № 149/7/2/6-432 «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности»;

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

5. Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

6. Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

7. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

8. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

9. Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

5 Практическое занятие № 5. Обследование критической информационной инфраструктуры в соответствии с ФЗ № 187. Категорирование объектов критической информационной инфраструктуры

Форма проведения практического занятия:

– первая часть занятия проводится в виде опроса и рассмотрением задач (ситуаций).

– вторая часть занятия проводится в виде выполнения РГЗ.

Цель занятия:

Изучить нормативно-методическую базу в области защиты КИИ, изучить методику категорирования объектов критической информационной инфраструктуры.

Вопросы для опроса:

1. Основные направления госполитики в области обеспечения безопасности АСУ П и ТП КВО инфраструктуры РФ. ФЗ № 187 от 26.07.2017 «О безопасности КИИ РФ».

2. Меры по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак.

3. Что такое ГосСОПКА?

4. Правила категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений.

5. Правила осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ.

6. Требования к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования. О Национальном координационном центре по компьютерным инцидентам (НКЦКИ).

7. Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ.

РГЗ - Категорирование объектов критической информационной инфраструктуры

Цель РГЗ: овладеть навыками категорирования объектов КИИ, научаться заполнять документацию КИИ, в соответствии с требованиями нормативно-методической базой ФСТЭК и ФСБ.

Для выполнения РГЗ необходимо выбрать объект КИИ для исследования. Объект выбирается учащимся самостоятельно, либо выдаётся преподавателем.

Согласно ФЗ-187, к объектам КИИ могут быть отнесены информационные системы и сети, а также автоматизированные системы управления, функционирующие в сфере:

- здравоохранения;
- науки;
- транспорта;
- связи;
- энергетики;
- банковской и иных сферах финансового рынка;
- топливно-энергетического комплекса;
- атомной энергии;
- оборонной и ракетно-космической промышленности;
- горнодобывающей, металлургической и химической промышленности.

Объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия между ними, составляют понятие критической информационной инфраструктуры.

Ход выполнения работы:

1. Скачайте программу «Обследование критической информационной инфраструктуры в соответствии с ФЗ № 187» https://ufer.osu.ru/index.php?option=com_uferdbsearch&view=uferdbsearch&action=details&ufer_id=1698

2. Откройте программу «Обследование критической информационной инфраструктуры в соответствии с ФЗ № 187». Прикладная программа «Автоматизированная система категорирования объектов критической информационной инфраструктуры» позволяет присвоить объекту критической информационной инфраструктуры категорию в зависимости от введенных значений, а также сформировать на основе полученных данных форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий.

3. Для запуска программы дважды кликните на «CategorizeObjects.exe» в папке «Release», появится основное окно программы.

Окно «Сведения о субъекте критической информационной инфраструктуры» содержит в себе текстовые поля и соответствующие им названия. Данные поля необходимо заполнить для того, чтобы в дальнейшем передать эту информацию в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий. Нет необходимости заполнять все поля, т.к. их можно будет отредактировать в готовом документе.

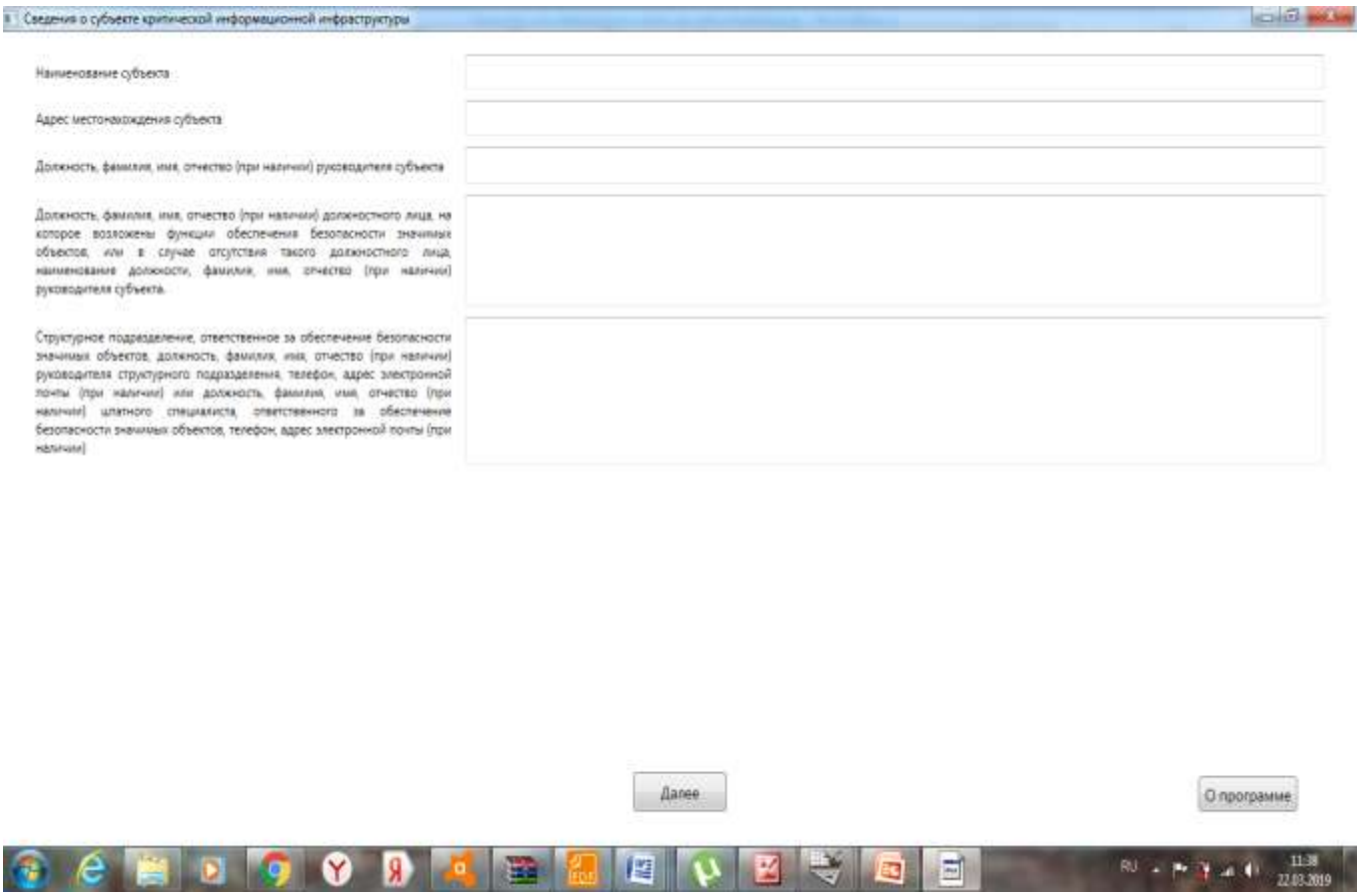

Рисунок 5.1 – Основное окно программы

2. При нажатии на кнопку «Далее» происходит переход в окно «Сведения об объекте критической информационной инфраструктуры». Заполните информацию о выбранном Вами объекте. В верхней части окна находятся следующие вкладки: «Объект», «Электросвязь», «Эксплуатирующее лицо», «Программы», «Сведения об угрозах», «Последствия компьютерных инцидентов», «Организационные и технические меры» и «Показатели критериев значимости». Во всех, кроме последней вкладки, содержатся текстовые поля и соответствующие им названия. Данные поля необходимо заполнить для того, чтобы в дальнейшем передать эту информацию в форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий. Нет необходимости заполнять все поля, т.к. их можно будет отредактировать в готовом документе.

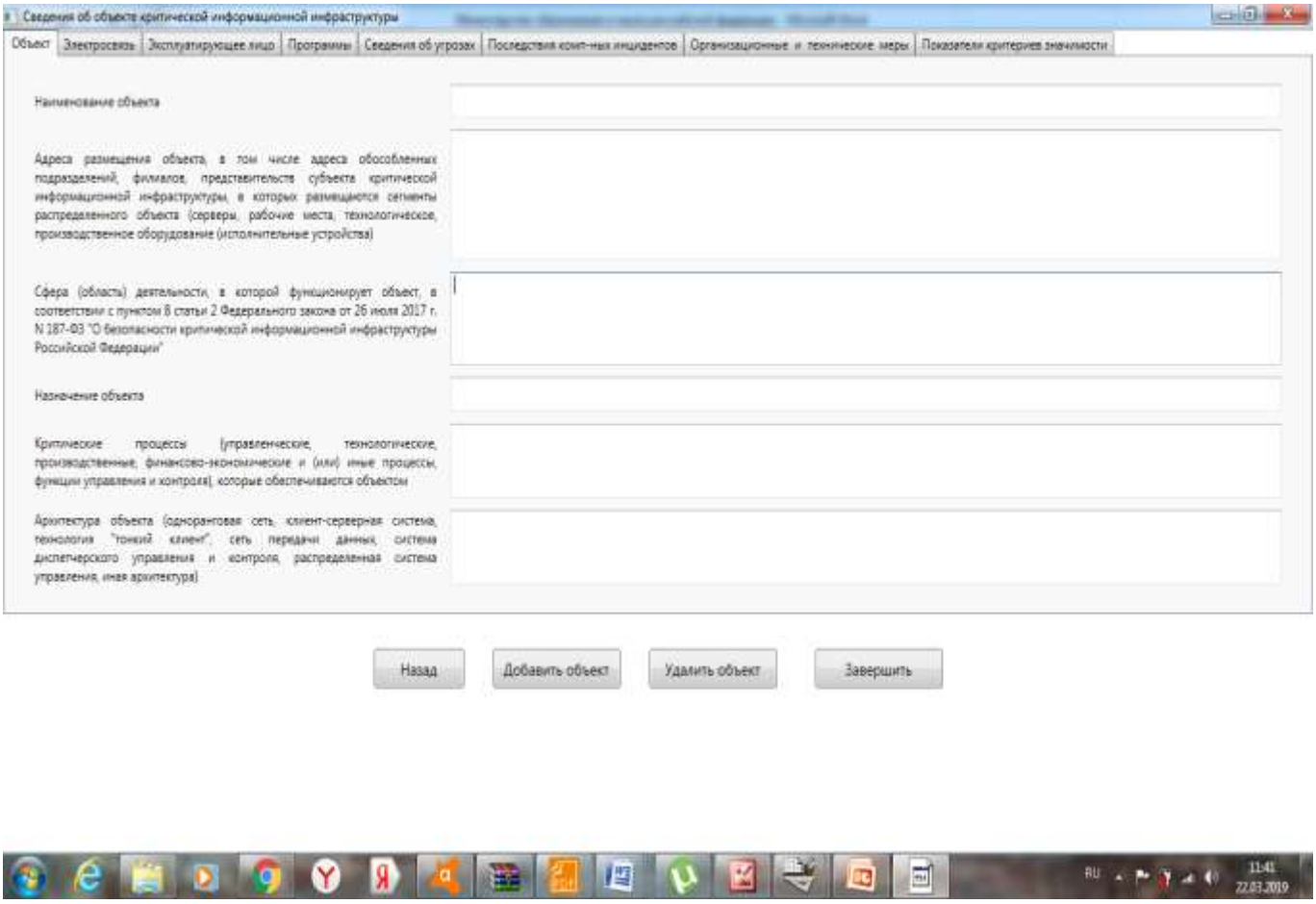

Рисунок 5.2 - Сведения об объекте критической информационной инфраструктуры

3.Во вкладке «Показатели критериев значимости» содержатся 5 показателей критериев значимости. Чтобы заполнить значения полей соответствующего критерия надо поставить галочку рядом с названием (рисунок 4). Пользователь выбирает только те критерии, которые ему нужны. Но в выбранном критерии необходимо заполнить все поля, иначе появится окно с сообщением об ошибке. Текстовые поля заполняются допустимыми числовыми значениями, согласно постановлению от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», а для остальных выбрать значения из выпадающего списка.

Для просмотра вышесказанного документа нужно нажать на ссылку внизу окна «Сведения об объекте критической информационной инфраструктуры» во вкладке «Показатели критериев значимости».

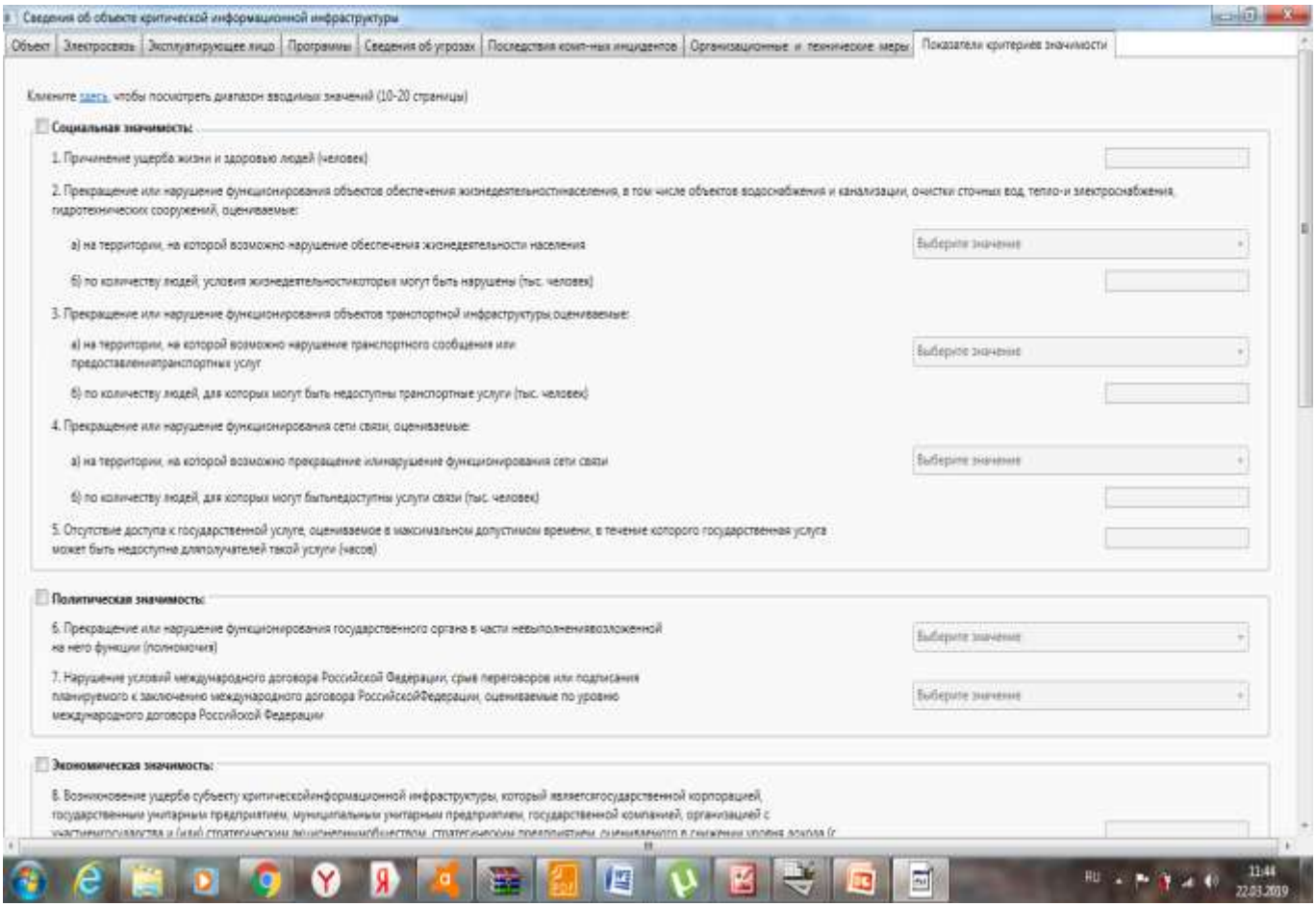

Рисунок 5.3 - Показатели критериев значимости

В нижней части окна расположены 4 кнопки: «Назад», «Добавить объект», «Удалить объект» и «Завершить». При клике на кнопку «Назад» происходит возврат в предыдущее окно. Для добавления нового объекта необходимо нажать на «Добавить объект». После этого откроется новое окно как на рисунке 3. Если Вы хотите удалить данный объект, надо нажать кнопку «Удалить объект».

После заполнения всей необходимой информации, нажмите на кнопку «Завершить».

Напротив каждого объекта размещена кнопка «Предварительный просмотр», при клике на которую откроется временный файл с расширением «docx» с заполненной информацией о субъекте и объекте (объектах).

Для сохранения интересующих данных об объекте в файл, необходимо поставить галочку рядом с соответствующим названием объекта и нажать на кнопку «Сохранить» в нижней части окна. После откроется диалоговое окно с выбором места для сохранения папки «КИИ» с сформированными документами. В этой папке для каждого выбранного объекта создается папка с именем соответствующего объекта, в которой находятся два файла с расширением «docx». Первый называется, как и сам объект и содержит заполненную форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий. Второй файл «Рекомендации.docx» содержит минимальных набор показателей по классам защищенности средств вычислительной техники и средств защиты информации.

4. Проанализируйте все полученные данные.

Список источников для самоподготовки

1. ФЗ № 187 от 26.07.2017 «О безопасности КИИ РФ»;
2. Указ Президента РФ № 569 от 25.11.2017 «О внесении изменений в Положение о ФСТЭК»;
3. Указ Президента РФ № 620 от 22.12.2017 «О совершенствовании ГосСОПКА»;
4. Указ Президента РФ № 98 от 02.03.2018 «О внесении изменения в перечень сведений, отнесенных к гостайне»;
5. Указ Президента РФ № 31с от 15.01.2013 «О создании ГосСОПКА»;
6. Указ Президента РФ № К1274 от 12.12.2014 «О Концепции ГосСОПКА»;
7. Постановление Правительства РФ № 127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»;

8. Постановление Правительства РФ № 162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»;

9. Постановление Правительства РФ № 808 от 11.07.2018 «О внесении изменения в Правила организации повышения квалификации специалистов по ЗИ и должностных лиц, ответственных за организацию ЗИ в ОГВ, ОМС, организациях с госучастием и организациях ОПК»;

10. Приказ ФСТЭК России № 227 от 06.12.2017 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ»;

11. Приказ ФСТЭК России № 229 от 11.12.2017 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»;

12. Приказ ФСТЭК России № 235 от 21.12.2017 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»;

13. Приказ ФСТЭК России № 236 от 22.12.2017 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

14. Приказ ФСТЭК России № 239 от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»;

15. Приказ ФСТЭК России № 72 от 26.04.2018 «О внесении изменений в Регламент ФСТЭК»;

16. Приказ ФСТЭК России № 138 от 09.08.2018 «О внесении изменений в Требования к обеспечению ЗИ в АСУ П и ТП на КВО, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК №31, и в Требования по обеспечению безопасности ЗО КИИ РФ, утвержденные приказом ФСТЭК № 239»;

17. Приказ ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам (НКЦКИ)»;

18. Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»;

19. Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

20. Проект приказа ФСБ России «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»;

21. Проект приказа ФСБ России «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»;

22. Проект приказа ФСБ России «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ»;

23. Рекомендации № 149/2/7-200 от 24.12.2016 «Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА»;

24. «Временный порядок включения корпоративных центров в ГосСОПКА» Информационное сообщение ФСТЭК России № 240/22/2339 от 04.05.2018 «О методических документах по вопросам обеспечения безопасности информации в КСИИ РФ»;

25. Информационное сообщение ФСТЭК России № 240/25/3752 от 24.08.2018 «По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

6 Практическое занятие № 6. Режим защиты государственных информационных систем. Построение системы защиты ГИС

Форма проведения практического занятия:

– первая часть занятия проводится в виде опроса и рассмотрением задач (ситуаций).

– вторая часть занятия проводится в виде выполнения РГЗ.

Цель занятия: изучить нормативно-правовую базу в области защиты ГИС.

Вопросы для опроса:

1. Порядок разработки, согласования и утверждения планов проведения мероприятий по защите государственных информационных систем.

2. Создание и функционирование системы защиты информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий.

3. Стадии и этапы создания системы защиты государственных информационных систем (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации на соответствие требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации).

4. Разработка эксплуатационной документации на систему защиты информации.

РГЗ - Построение системы защиты ГИС

Цель РГЗ: научиться формировать частную модель угроз и нарушителя для ГИС на основе нормативно-методических документов. Научиться формировать требования по защите ГИС.

Данное РГЗ основано на данных РГЗ - Методика определения актуальных угроз в ИСПДн. Требования к системе защиты ИСПДн.

Ход выполнения работы:

1. Откройте данные полученные в РГЗ - Методика определения актуальных угроз в ИСПДн. Требования к системе защиты ИСПДн. Объект, исследования ваша ИСПДн, которая принадлежит государственной организации.

2. Откройте Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о ЗИ, не составляющей ГТ, содержащейся в ГИС». Определите уровень значимости информации вашего объекта. Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации. УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)].

3. На основе приказа определите масштаб ГИС. Информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях. Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях. Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях.

4. Определите класс защищенности ГИС

Таблица 6.1 – Класс защищенности ГИС

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Муниципальный	Объектовый
УЗ1	К1	К1	К1
УЗ2	К2	К2	К2
УЗ3	К3	К3	К3

5. Определите Состав мер защиты информации и их базовые наборы для класса защищенности информационной системы вашего объекта.

6. Осуществите выбор средств обеспечения безопасности информации в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о ЗИ, не составляющей ГТ, содержащейся в ГИС», используя Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00).

Таблица 6.2 – Классы средств защиты информации для ГИС

Средства защиты информации		ИС 1 и 2 класса защищенности	ИС 3 класса защищенности	ИС 4 класса защищенности
Средства вычислительной техники		Не ниже 5 класса	Не ниже 5класса	Не ниже 5класса
Системы обнаружения вторжений и средства антивирусной защиты	Есть интернет	Не ниже 4 класса	Не ниже 4класса	Не ниже 5класса
	Нет интернета		Не ниже 5класса	
Межсетевые экраны	Есть интернет	Не ниже 3 класса	Не ниже 3 класса	Не ниже 4 класса
	Нет интернета	Не ниже 4 класса	Не ниже 4 класса	

Список источников для самоподготовки

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

2. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

3. Информационное сообщение от 22 июня 2017 г. № 240/22/3031 О порядке рассмотрения и согласования моделей угроз безопасности информации и технических заданий на создание государственных информационных систем;

4. Постановление Правительства Российской Федерации от 11 мая 2017 г. № 555 «О внесении изменений в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;

5. Методический документ ФСТЭК России от 11.02.2014. Меры защиты информации в государственных информационных системах;

6. Постановление Правительства РФ от 06.07.2015 № 676 О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации;

7. Приказ Минкомсвязи России от 11.08.2016 № 375 Об утверждении порядка внесения сведений о выполнении требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, а также состава сведений, которые подлежат внесению, и срока их представления;

8. Приказ Роскомнадзора от 20.10.2017 № 213 Об утверждении Требований к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования федеральной государственной информационной системой информационных ресурсов,

информационно-телекоммуникационных сетей, доступ к которым ограничен на территории Российской Федерации в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации»;

9. Приказ ФСТЭК России от 15.02.2017 г. № 27 О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 г. № 17.

7 Практическое занятие № 7. Аттестация объектов информатизации по требованиям безопасности информации. Лицензирование и система сертификации средств защиты информации

Форма проведения практического занятия:

– первая часть занятия проводится в виде опроса и рассмотрением задач (ситуаций).

– вторая часть занятия проводится в виде выполнения и защиты реферата.

Цель работы:

Закрепление теоретических знаний по вопросам аттестации объектов информатизации по требованиям безопасности информации, закрепление теоретических знаний по вопросам государственного лицензирования деятельности в области защиты информации.

Вопросы для опроса:

1. Перечень видов деятельности, на осуществление которых требуется лицензия.
2. Органы, уполномоченные на ведение лицензионной деятельности.
3. Основные принципы, организационная структура и порядок проведения аттестации.
4. Какие объекты информатизации подлежат обязательной аттестации.
5. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации. Орган по аттестации. Порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации. Правовой статус аттестата соответствия. Подача апелляции.

6. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности информации.

7. Анализ исходных данных по аттестуемому объекту информатизации; предварительное ознакомление с аттестуемым объектом информатизации. Проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации.

8. Проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств; проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации.

9. Проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации. Анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

10. Документация, сопровождающая аттестационные испытания. Заявка на проведение аттестации объекта информатизации. Аттестат соответствия требованиям безопасности информации. Типовая форма акта классификации. Типовая форма матрицы доступа. Рекомендуемые формы приказов. Инструкция по учету лиц. Рекомендуемая форма модели угроз. Типовая форма требований по обеспечению безопасности персональных данных. Типовая форма журнала учета средств защиты информации. Типовая форма заключения о возможности эксплуатации средств защиты информации. Типовая форма инструкции по организации резервирования. Типовая форма журнала учета машинных носителей. Типовая форма акта обследования. Типовая форма заключения по результатам аттестационных испытаний. Типовая форма описания системы защиты. Типовая форма аттестата соответствия. Перечень вопросов по обеспечению безопасности персональных данных.

11. Эксплуатация аттестованных объектов информатизации. Переаттестация. Ответственность владельца аттестованного объекта информатизации. Действия в случае изменения условий и технологий обработки защищаемой информации. Осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации. Приостановление или аннулирование действие аттестата соответствия.

12. Организационная структура системы государственного лицензирования в области защиты информации.

13. Общий порядок проведения лицензирования в области защиты информации.

14. Контроль за деятельностью лицензиатов.

15. Изучение перечня видов деятельности предприятий в области защиты информации, подлежащих лицензированию.

16. Сформулируйте основные понятия, принятые в сфере государственного лицензирования в области защиты информации.

17. Организационная структура системы государственного лицензирования в области защиты информации.

18. Функции государственных органов по лицензированию в области защиты информации.

19. Функции лицензионных центров по лицензированию в области защиты информации.

20. Права и обязанности лицензиатов.

21. Порядок проведения лицензирования и контроля за деятельностью лицензиатов.

22. Назовите случаи приостановления или прекращения действия лицензии.

23. В каких случаях предприятию отказывают в выдаче лицензии?.

24. Какие документы предоставляются для получения лицензии?

25. Каковы особенности лицензирования деятельности по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?

26. Какие средства относятся к шифровальным?

27. Каковы особенности лицензирования видов деятельности, связанных с шифровальными (криптографическими) средствами?

28. Назовите лицензионные требования и условия при распространении шифровальных (криптографических) средств.

29. Назовите лицензионные требования и условия при осуществлении разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.

30. Назовите лицензионные требования и условия при предоставлении услуг в области шифрования информации.

31. Назовите лицензионные требования и условия при осуществлении деятельности по техническому обслуживанию шифровальных (криптографических) средств.

Темы рефератов:

1. Лицензирование деятельности в области защиты государственной тайны.
2. Особенности лицензирования деятельности в области защиты информации, составляющей государственную тайну.
3. Общий порядок проведения лицензирования в области защиты информации.
4. Система сертификации средств защиты информации по требованиям безопасности информации.
5. Система сертификации средств криптографической защиты информации
6. Виды аттестации помещений по требованиям безопасности информации.

Список источников для самоподготовки

1. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Гостехкомиссией РФ 25.11.1994);

2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения;

3. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения;

4. Постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

5. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»;

6. Постановление Правительства Российской Федерации от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности»;

7. Постановление Правительства РФ от 29 декабря 2007 г. № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;

8. Приказ ФСТЭК России от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации».

8 Практическое занятие № 8. Ответственность за правонарушения в области информационной безопасности

Форма проведения практического занятия:

– первая часть занятия проводится в виде опроса и рассмотрением задач (ситуаций).

– вторая часть занятия проводится в виде выполнения и защиты реферата.

Цель занятия:

Изучить основные статьи по правонарушениям в области информационной безопасности уголовного, административного, и трудового кодексов.

Вопросы для опроса:

1. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.
2. Меры дисциплинарной ответственности.
3. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности.
4. Уголовная ответственность за правонарушения в области конфиденциальной информации.

Темы рефератов:

1. Понятие и виды юридической ответственности за нарушение правовых норм по защите информации.
2. Меры дисциплинарной ответственности согласно Трудового кодекса РФ.
3. Административная ответственность за правонарушения в области защиты интеллектуальной собственности и информационной безопасности.
4. Уголовная ответственность за правонарушения в области конфиденциальной информации.

Список источников для самоподготовки

1. Гражданский кодекс Российской Федерации (ГК РФ);
2. Трудовой кодекс Российской Федерации (ТК РФ);
3. Кодекс об административных правонарушениях (КоАП РФ);
4. Уголовный кодекс Российской Федерации (УК РФ).