МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный университет экономики и управления «НИНХ»
(ФГБОУ ВО «НГУЭУ», НГУЭУ)

Кафедра информационной безопасности

Рег. № 4191-17/02

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ КУРСОВОЙ РАБОТЫ

ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление:
10.03.01 Информационная безопасность

Направленность (профиль):
Организация и технология защиты информации (в государственном и частном секторе)

Новосибирск 2017

Методические указания по выполнению курсовой работы разработаны
Селифановым Валентином Валерьевичем, ст. преподавателем кафедры информационной безопасности

Методические указания по выполнению курсовой работы прошли экспертизу УМУ

Утверждено на заседании кафедры Информационной безопасности
(протокол от «30» августа 2017 г. № 1).

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ЦЕЛИ И ЗАДАЧИ ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Цель курсовой работы заключается в закреплении знаний в области организационно-правового обеспечения защиты информации и приобретение ими практических навыков самостоятельной аналитической (исследовательской) работы по аудиту информационных ресурсов, классификации автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, классификации информационных систем.

Задачи курсовой работы:

– закрепление базовых понятий защиты прав субъектов персональных данных и обеспечения безопасности персональных данных;

– углубление понимания положений закона «О персональных данных», соответствующих ему Постановлений правительства РФ от 01.11.2012 № 1119 и Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17, Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным приказом ФСТЭК России от 18 февраля 2013 г. № 21, Требований к обеспечению защиты информации, обработка которой осуществляется автоматизированными системами управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденных приказом ФСТЭК России от 14 марта 2014 г. № 31;

– получение навыков в разработке внутренних организационных документов по защите информации.

–

РАЗДЕЛ 2. ИНСТРУКЦИЯ ПО ВЫПОЛНЕНИЮ КУРСОВОЙ РАБОТЫ

Студенты выполняют курсовые работы по единой теме «Защита автоматизированных (информационных) систем» с выбором конкретного объекта из списка вариантов, предложенных преподавателем. Для исследования в рамках курсовой работы студентам могут быть предложены следующие виды объектов: автоматизированные системы (АС), государственные информационные системы (ГИС), информационные системы персональных данных (ИСПДн), автоматизированные системы управления технологическими процессами (АСУ ТП).

Курсовая работа включает следующие четыре типовых задания, адаптированных для выбранного варианта объекта.

1. Согласно варианта Приложение Е–Оформить один или несколько необходимых документов (виды и количество документов зависит от выбранного варианта объекта): «Акт классификации АС», «Акт определения уровня защищенности ИСПДн», «Акт классификации государственной ИС», «Акт классификации АСУ ТП».

2. Для каждой угрозы, приведенной в Типовой модели (Приложение Е), в соответствии с вариантом, привести 3 примера угроз с описанием в соответствии с Приказом № 17 (использовать электронный ресурс bdu.fstec.ru).

3. Выбрать для ИС в соответствии с вариантом (Приложение Е) построить уточненный базовый набор мер, используя Методический документ ФСТЭК России «Меры защиты информации в ГИС»

4. Сформировать и обосновать требования к средствам защиты для каждой меры и привести примеры соответствующих средств защиты информации.

Выполнение курсовой работы состоит из следующих этапов: 1) выбор варианта курсовой работы; 2) решение основных задач курсовой работы; 3) оформление работы; 4) представление и защита работы.

Этап 1. Выбор варианта работы.

Цель этого этапа – выбор объекта с уточнёнными параметрами и фиксация варианта курсовой работы распоряжением заведующего кафедрой по представлению преподавателя дисциплины. Примерный список объектов с кратким описанием приведён в приложении 1. В соответствии с выбранным вариантом составляется задание на курсовую работу и календарный план (график) её выполнения. Преподаватель консультирует студента по вопросам, которые касаются выбора варианта курсовой работы.

Вариант курсовой работы определяется в течение 1 месяца от начала семестра. В этом же срок должны быть составлены и подписаны задание на курсовую работу и календарный план.

Этап 2. Решение основных задач курсовой работы.

Цель этапа - получение основных результатов курсовой работы в соответствии с общей структурой задания на курсовую работу и индивидуальным заданием, сформированным в соответствии с выбранным вариантом. Этот этап подразделяется на несколько шагов.

Шаг 1. Составление Актов. Углублённое изучение нормативно-правовых документов, регламентирующих организацию защиты информации в условиях, соответствующих выбранному варианту. В соответствии с ними должны быть составлены шаблоны Актов, разработка которых предусмотрена п.1. типового задания, описанного выше (стр. 4). В завершение данного этапа необходимо сопоставить вид объекта и условия его функционирования с требованиями отобранных нормативно-правовых документов, после чего заполнить подготовленные шаблоны конкретными данными, относящимися к выбранному варианту.

Шаг 2. Анализ угроз. На этом шаге нужно изучить Типовую модель …. (Приложение Е) и банк данных угроз, разработанный ФСТЭК России (далее - БДУ) и размещённый на ресурсе http://www.bdu.fstec.ru. Изучить структуру описании угроз и уязвимостей на данном ресурсе, соотнести их со структурой угроз в Типовой модели. Опираясь на Типовую модель, отобрать три угрозы, характерные для объекта своего варианта. Проанализировать каждую из этих угроз и составить её характеристику в соответствии со структурой угроз в БДУ.

Шаг 3. Выбор базового и уточненного набора мер. На данном шаге вначале составляется базовый набор мер, который определяется классом и (или) уровнем защищённости. На основе него в соответствии с Методическим документом ФСТЭК России «Меры защиты информации в ГИС» строится и обосновывается уточнённый набор мер, который и является результатом данного шага. Следует обратить внимание на необходимость обоснований по каждой исключённой (добавленной) мере в процессе перехода от базового к уточнённому набору мер.

Шаг 4. Выбор средств защиты. Для выполнения данного шага в соответствии с требованиями нормативно-правовых документов ФСТЭК России следует определить рекомендуемый состав средств защиты информации и требования к классам их защищённости в соответствии результатами классификации объекта исследования. После этого проанализировать реестр сертифицированных средств защиты информации и выбрать несколько примеров средств по каждой позиции, подходящие под список требований.

Этап 3. Оформление курсовой работы .

Курсовая работа оформляется в соответствии с Порядком оформления письменных работ обучающихся. Процесс оформления курсовой работы рекомендуется начать после получения темы и сразу оформить шаблон документа с соблюдением требований к форматированию в соответствии с Порядком оформления письменных работ и представленными в приложениях шаблонами титульного листа и сопроводительной документации. Далее написание текста курсовой работы удобно вести параллельно выполнению работ этапа 2. Каждый шаг второго этапа, в целом, соответствует содержанию очередного раздела: Шаг 1 – введение и раздел 1, шаг 2 – раздел 2, шаг 3 – раздел 3, шаг 4 – раздел 4. По окончании работ следует написать заключение, оформить заявление о

самостоятельном выполнении курсовой работы (ПРИЛОЖЕНИЕ Г), проверить текст через систему «антиплагиат», чтобы убедиться, что объём оригинального текста составляет не менее 70%.

После завершения работы над текстом КР нужно заполнить ФИО студента, группу и дисциплину в рецензии на курсовую работу (приложение Д). Электронный вариант отправляется преподавателю по электронной почте (или через систему MOODLe). Печатный и электронный варианты предоставляется на кафедру (при наличии электронного ресурса по дисциплине в MOODLe загружается в систему). Более подробно требования к структуре и содержанию КР приведены ниже в разделе 3.

Этап 4. Представление и защита курсовой работы

Представление и защита работы проводится студентом в публичной или индивидуальной форме (по решению преподавателя). Для представления работы студенту нужно подготовить доклад на 6-7 минут. Во время доклада студент:

- представляет вариант выбранного объекта;
- обосновывает акт классификации;
- аргументирует результаты анализа угроз;
- обосновывает сформированный список требований к составу средств защиты информации, их характеристикам и сертификатам;
- представляет выбранный в итоге комплект средств защиты информации с необходимой аргументаций выбора конкретных средств из разных вариантов.

После доклада студент отвечает на вопросы преподавателя и, в случае публичной защиты, других студентов. Далее эти замечания могут быть учтены при доработке курсовой работы.

График докладов составляется преподавателем в течение последнего месяца обучения в 5 семестре.

Оценка за курсовую работу выставляется преподавателем после проверки её электронной и печатной версий с учётом качества написания текста курсовой работы и доклада на представлении результатов. При необходимости (например, при большом объёме доработок) преподаватель может повторно заслушать студента после доработки курсовой работы перед выставлением оценки.

Порядок работы с литературой

Работа с учебно-методической литературой, нормативно-правовыми и информационно-справочными источниками играет важную роль для написания качественной курсовой работы. Основной теоретический материал даётся на лекциях и практических занятиях, однако при написании курсовой работы необходимо более детальный анализ нормативных правовых документов. Важной частью является работа с БДУ ФСТЭК России – официальным универсальным источником информации об актуальных угрозах и уязвимостях. Литературные источники, рекомендованные в рабочей программе дисциплины, позволяют дополнительно проработать теоретическую базу, закрепить знание терминологии и нормативно-правовой основы, разобраться.

При выборе источников в сети Интернет можно использовать только доверенные электронные ресурсы (электронные библиотечные системы, сайты органов власти, справочно-правовые системы, сайты производителей средств защиты информации, электронные научные и информационно-справочные журналы, авторитетные специализированные порталы по тематике и др.) – основные такие ресурсы рекомендованы в рабочих программах дисциплин, в случае затруднений рекомендуется обратиться к преподавателю за консультаций. На все используемые источники должны быть даны ссылки их текста курсовой работы.

РАЗДЕЛ 3. ТРЕБОВАНИЯ К СТРУКТУРЕ И СОДЕРЖАНИЮ КУРСОВОЙ РАБОТЫ

Курсовая работа должна иметь следующую структуру:

- титульный лист;
- заявление о самостоятельном характере выполненной работы;
- задание на курсовую работу
- содержание;
- введение;
- основная часть, состоящая из разделов и параграфов;
- заключение;
- список использованных источников;
- приложения.

По тем позициям, которые не отражены в настоящих методических указаниях, оформление курсовой работы должно выполняться в соответствии с требованиями внутреннего стандарта НГУЭУ по оформлению письменных работ студентов.

Общий объем работы без приложений 15-25 страниц

Титульный лист и задание

Титульный лист оформляется в соответствии с Приложением Б. заполнить распечатать и подписать у преподавателя задание на курсовую работу (Приложение В). Содержание включает порядковые номера и наименования основных разделов (при необходимости подразделов) работы, приложений с указанием их обозначения и заголовков, номера страниц. Рекомендуется создавать автоматически, корректируя при необходимости шрифты.

Списки сокращений, терминов и определений

Размещают перед введением. Для англоязычных терминов указывают также и их русскоязычные эквиваленты. Для англоязычных аббревиатур указывают их расшифровку на английском языке, и пояснение на русском. В список терминов и определений (глоссарий) включают основополагающие термины по защите информации, используемые в работе, особенно те, относительно которых имеются различные толкования в нормативно-правовой и учебно-методической литературе (термины, не используемые в работе, в глоссарий не включаются). При формировании глоссария нужно опираться на законы, ГОСТы, официальные нормативно-методические документы, материалы лекций, авторитетные учебные издания. При необходимости следует проконсультироваться у преподавателя. В глоссарий также включают специфические или малораспространенные термины, касающиеся предметной области и используемых технологий. Сокращения, внесенные в список сокращений, далее по тексту не раскрываются. При наличии списка сокращений в него должны быть включены все сокращения, встречающиеся в работе.

Введение

Введение не нумеруют и размещают на отдельном листе. Во введении даётся краткое описание объекта в соответствии с выбранным вариантом, формулируется цель курсовой работы, и определяются решаемые задачи. Объем введения не менее одного полного листа, не более 2 листов. Если на листе концовка введения (или другого раздела) занимает всего несколько строчек, и далее – пустой лист, то текст надо либо сократить до полной страницы либо дополнить не менее, чем до половины страницы.

Основная часть

Основная часть содержит подробное описание объекта исследования. Структура основной части соответствует основным этапам работы. Целесообразно включать в неё следующие разделы и параграфы.

Первый раздел – характеристика нормативно-правовой базы, регулирующей объект, исследуемый в соответствии с выбранным вариантом, обоснование акта (актов) классификации и ссылку на приложения, в которых приводятся соответствующие разработанные документы.

Второй раздел содержит материалы, касающиеся анализа угроз в соответствии с п.2 типового задания, необходимыми обоснованиями и ссылками на нормативно-правовые документы, акт классификации и электронный ресурс БДУ.

В третьем разделе обосновывается процесс формирования базового и уточнённого набора требований к защите информации для заданного объекта и формулируется итоговый список требований.

Четвертый раздел включает материалы, аргументирующие выбор средств защиты информации в соответствии с требованиями, сформулированными в третьем разделе, и список выбранных в итоге средств.

При написании курсовой работы необходимо придерживаться стиля научно-технической работы, особенности которого приведены во внутреннем стандарте НГУЭУ по оформлению письменных работ.

Все заимствования в тексте курсовой работы (цитирования) должны быть корректно оформлены и иметь ссылки на соответствующие источники.

Перед передачей работы на проверку преподавателю текст должен быть проверен с использованием системы «Антиплагиат» и заполнено заявление о самостоятельном характере выполненной работы.

Соответствующий протокол представляется вместе с работой. В сомнительных случаях преподаватель проводит дополнительную проверку работы на предмет наличия плагиата.

Заключение

Как и введение, заключение не нумеруют. Его объем должен составлять не менее одной полной страницы и не более двух страниц. В заключении даётся сжатое резюме выполненной работы (методы и особенности решения поставленных задач), перечисляются полученные результаты и формулируются выводы по итогам проделанной работы.

Список литературы

В список литературы включают все использованные при выполнении курсовой работы источники. Список дают в соответствии с ГОСТ 7.1.84. Примеры оформления списка литературы приведены во внутреннем стандарте НГУЭУ по оформлению письменных работ.

Список литературы должен включать необходимые законы и другие нормативно-правовые акты, ГОСТы и иные стандарты, а также необходимые интернет-источники, учебную, методическую и научную литературу.

На все источники должны быть ссылки из текста.

Приложения

Материал, дополняющий содержание курсового проекта размещают в приложениях. Это могут быть акты классификации, аналитические таблицы большого формата, графические и справочные материалы, другая документация. На все приложения должны быть ссылки из текста курсовой работы.

РАЗДЕЛ 4. ПОКАЗАТЕЛИ, КРИТЕРИИ И ШКАЛА ОЦЕНКИ КУРСОВОЙ РАБОТЫ

При оценке курсовой работы учитываются следующие показатели.

Показатель	Краткая характеристика оцениваемых качеств курсового проекта	Макс. число баллов
1.Содержание	Обоснование актуальности; корректность постановки цели и задач; соответствие результатов цели и задачам; логичность структуры и изложения, отсутствие противоречий; полнота охвата материала в пределах поставленных задач; аргументированность выводов; обоснованность используемых методов и технологических решений; корректность применения профессиональных знаний и методов; качество графического материала (схемы, рисунки) и его соответствие тексту; обоснованность подбора учебно-научной литературы и информационных источников (кол-во источников – не менее 10); корректность цитирований и соблюдение требований по антиплагиату.	40 баллов
2.Защита	Качество устного сообщения (доклада и презентации), полнота и профессионализм ответов на вопросы, в т.ч. по замечаниям к тексту курсового проекта.	20 баллов
3.Оформление	Соблюдение стиля научно-технического текста, грамотность, правильное оформление ссылок на используемую литературу и другие информационные	20 баллов

	источники, аккуратное форматирование, соответствие требованиям стандарта оформления письменных работ.	
4.График	Соблюдение календарного плана, баллы снижаются при предоставлении КР (-5 баллов за неделю).	20 баллов

ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ

Тема курсовой работы: «Автоматизированные системы в защищенном исполнении.»

ВАРИАНТЫ КУРСОВОЙ РАБОТЫ

№ п/п	Количество пользователей	Уровень доступа	Уровни конфиденциальности	Тип угроз	Вид ИСПДн	Масштаб ГИС	Уровень значимости	Типовая модель угроз	Степень ущерба АСУ ТП
1.	>2	Одинаковый	2	1	С	Ф	1	2	Высокая
2.	1	-	3	2	О	Р	2	1	Средняя
3.	>2	Разный	2	3	Б	О	3	3	Низкая
4.	>2	Разный	3	1	И	Ф	4	4	Высокая
5.	>2	Одинаковый	2	2	С	Р	1	5	Средняя
6.	>2	Разный	3	3	И	О	2	5	Низкая
7.	>2	Одинаковый	3	1	И	Ф	3	4	Высокая
8.	>2	Разный	2	2	С	Р	4	3	Средняя
9.	>2	Одинаковый	3	3	И	О	1	2	Низкая
10.	>2	Разный	2	1	С	Р	2	1	Высокая
11.	>2	Одинаковый	3	2	Б	О	3	3	Средняя
12.	1	-	2	3	О	Ф	4	1	Низкая
13.	>2	Разный	3	1	С	О	1	4	Высокая
14.	>2	Одинаковый	1	2	И	Ф	2	5	Средняя
15.	>2	Разный	2	3	С	Р	3	2	Низкая
16.	>2	Разный	3	1	И	О	1	2	Высокая
17.	>2	Одинаковый	2	2	С	Ф	2	3	Средняя
18.	1	-	2	3	Б	О	3	1	Низкая
19.	>2	Разный	2	1	И	О	1	3	Высокая
20.	>2	Одинаковый	3	2	С	О	2	4	Средняя
21.	>2	Разный	2	3	И	Р	3	3	Низкая
22.	>2	Разный	3	1	С	Ф	1	3	Высокая
23.	1	-	2	2	Б	Р	2	1	Средняя
24.	>2	Одинаковый	3	3	И	О	3	2	Низкая

1. Типовая модель угроз безопасности персональных данных обрабатываемых в автоматизированных рабочих местах, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена

При обработке ПДн на автоматизированном рабочем месте, имеющим подключения к сетям связи общего пользования и (или) сетям международного информационного обмена возможна реализация следующих УБПДн:

угрозы утечки информации по техническим каналам;

угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

угрозы утечки акустической (речевой) информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналу ПЭМИН.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теме же условиями и факторами, что и для автоматизированного рабочего места, не имеющего подключения к сетям связи общего пользования и (или) сетям международного информационного обмена.

Угрозы НСД в ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в

ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям общего пользования. Угрозы из внешних сетей включают в себя:

угрозы «Анализа сетевого трафика» с перехватом передаваемой в внешние сети и принимаемой из внешних сетей информации;

угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.;

угрозы выявления паролей;

угрозы получения НСД путем подмены доверенного объекта;

угрозы типа «Отказ в обслуживании»;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ.

2. Типовая модель угроз безопасности персональных данных обрабатываемых в локальных ИСПДн, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена

При обработке ПДн в локальных ИСПДн, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

угрозы утечки информации по техническим каналам;

угрозы НСД к ПДн, обрабатываемым в локальных ИСПДн.

Угрозы утечки информации по техническим каналам включают в себя:

угрозы утечки акустической (речевой) информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналу ПЭМИН.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теми же условиями и факторами, что и для локальных ИСПДн, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена.

Угрозы НСД в локальных ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн.

Угрозы НСД в ИСПДн, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место для отдельного АРМ, не подключенного к сетям общего пользования. Кроме того, в такой ИСПДн могут иметь место:

угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;

угрозы выявления паролей;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ.

3. Типовая модель угроз безопасности персональных данных обрабатываемых в локальных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена

При обработке ПДн в локальных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

угрозы утечки информации по техническим каналам;

угрозы НСД к ПДн, обрабатываемым в локальных ИСПДн.

Угрозы утечки информации по техническим каналам включают в себя:

угрозы утечки акустической (речевой) информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналу ПЭМИН.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теме же условиями и факторами, что и для предыдущих типов ИСПДн.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн, включают в себя угрозы, аналогичные тем, которые реализуются в локальной ИСПДн, не имеющей подключения к сетям общего пользования.

Угрозы из внешних сетей включают в себя:

угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации;

угрозы сканирования, направленные на выявление типа операционной системы ИСПДн, сетевых адресов рабочих станций, открытых портов и служб, открытых соединений и др.;

угрозы выявления паролей;

угрозы получения НСД путем подмены доверенного объекта;

угрозы типа «Отказ в обслуживании»;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ.

4. Типовая модель угроз безопасности персональных данных обрабатываемых в распределенных ИСПДн, не имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена

При обработке ПДн в распределенных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, возможна реализация следующих УБПДн:

угрозы утечки информации по техническим каналам;

угрозы НСД к ПДн, обрабатываемым в распределенных ИСПДн.

Угрозы утечки информации по техническим каналам включают в себя:

угрозы утечки акустической (речевой) информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналу ПЭМИН.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теме же условиями и факторами, что и для предыдущих типов ИСПДн.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн.

При этом могут быть угрозы, аналогичные тем, которые имеют место в локальной ИСПДн, не подключенной к сетям общего пользования, а также угрозы, реализуемые внутри распределенной сети с использованием протоколов межсетевого взаимодействия, в том числе:

угрозы «Анализа сетевого трафика» с перехватом передаваемой по сети информации;

угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.;

угрозы внедрения ложного объекта сети;

угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

угрозы выявления паролей;

угрозы типа «Отказ в обслуживании»;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ.

5. Типовая модель угроз безопасности персональных данных обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена

При обработке ПДн в распределенных ИСПДн, имеющих подключение к сетям связи общего пользования и (или) сетям международного информационного обмена возможна реализация следующих УБПДн:

угрозы утечки информации по техническим каналам;

угрозы НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Угрозы утечки информации по техническим каналам включают в себя:

угрозы утечки акустической (речевой) информации;

угрозы утечки видовой информации;

угрозы утечки информации по каналу ПЭМИН.

Возникновение УБПДн в рассматриваемых ИСПДн по техническим каналам характеризуется теме же условиями и факторами, что и для предыдущих типов ИСПДн.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующие угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена.

Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ИСПДн, аналогичны тем, которые имеют место в распределенных ИСПДн, не имеющей подключения к сетям общего пользования. Кроме того, в такой ИСПДн имеют место угрозы, реализуемые с использованием протоколов межсетевого взаимодействия из внешних сетей, в том числе:

угрозы «Анализа сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой в ИСПДн из внешних сетей информации;

угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;

угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;

угрозы подмены доверенного объекта;

угрозы навязывания ложного маршрута путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях;

угрозы выявления паролей;

угрозы типа «Отказ в обслуживании»;

угрозы удаленного запуска приложений;

угрозы внедрения по сети вредоносных программ.

ПРИЛОЖЕНИЕ Б

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Новосибирский государственный университет экономики и управления «НИНХ»
(ФГБОУ ВО «НГУЭУ», НГУЭУ)

Кафедра Информационной безопасности
(наименование кафедры)

КУРСОВАЯ РАБОТА

По дисциплине Организационно-правовое обеспечение информационной безопасности
(Наименование дисциплины)

Защита _____
(Наименование темы с учётом варианта объекта)

Ф.И.О студента _____
Направление/специальность 10.03.01. Информационная безопасность
Профиль: организация и технология защиты информации (в государственном и частном секторе)
Номер группы _____
Номер зачетной книжки _____
Дата регистрации курсовой работы кафедрой _____
Проверил _____

Новосибирск _____ *г.*

ПРИЛОЖЕНИЕ В

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный университет экономики и управления «НИНХ»
(ФГБОУ ВО «НГУЭУ», НГУЭУ)

Кафедра Информационной безопасности

ЗАДАНИЕ
на курсовую работу

Тема _____

ФИО студента _____

Группа _____

Перечень подлежащих разработке вопросов и календарный график

№ п/п	Наименование вопросов, подлежащих разработке (этапы работы)	Срок выполнения[1]
1.	Выбор темы курсовой работы. Краткая характеристика объекта. Обоснование актуальности - Введение.	До 1 октября
2	Анализ нормативно-правовой базы и разработка акта классификации - Раздел 1.	До 15 октября
3	Анализ угроз – Раздел 2.	До 5 ноября
4	Формирование уточнённого набора мер защиты информации – Раздел 3	До 20 ноября
5	Выбор средств защиты информации – Раздел 4.	До 5 декабря
6	Доклад по результатам работы	По графику в период с 5 по 15 декабря
7	Оформление и представление работы на проверку.	До 20 декабря
8	Доработка по замечаниям преподавателя (при необходимости). Итоговое собеседование. Выставление оценки	До 27 декабря

Дата выдачи задания «___» _____ 20 ___ года
Срок сдачи работы «___» _____ 20 ___ года
Преподаватель _____ _____
(фамилия и инициалы преподавателя) (подпись)

Задание получил студент _____ _____
(фамилия и инициалы студента) (подпись)

[1] Указаны примерные сроки. При заполнении задания для конкретных студентов даты могут быть скорректированы в зависимости от фактической даты получения задания.

ПРИЛОЖЕНИЕ Г

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный университет экономики и управления «НИНХ»
(ФГБОУ ВО «НГУЭУ», НГУЭУ)

Кафедра Информационной безопасности

ЗАЯВЛЕНИЕ
о самостоятельном характере выполненной работы

Я, _____
(Фамилия, имя, отчество)
Студент(ка) группы _____ , направления подготовки__ _____

_____,

направленности (профиля)_____,
заявляю, что в моей курсовой работе, выполненной на тему:
_____
_____,
не содержится элементов плагиата.

Все заимствования из печатных и электронных источников, а также из защищенных ранее письменных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

«_ __ _» _____ 20_ _ г. _____ И.О. Фамилия
(подпись)

Результаты проверки в системе «Антиплагиат»

Доля авторского текста (оригинальности) в результате автоматизированной проверки составила _____ %.

Руководитель курсовой работы _____
(уч. степень, должность, Фамилия И.О.)

«_ _____ _» _____ 20__ _ г. _____
(подпись)

ПРИЛОЖЕНИЕ Д

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный университет экономики и управления «НИНХ»
(ФГБОУ ВО «НГУЭУ», НГУЭУ)

Кафедра Информационной безопасности
(наименование кафедры)

РЕЦЕНЗИЯ
на курсовую работу

ФИО студента _____
Группа _____
Дисциплина _____

№ п/п	Критерии оценки	Оценочные баллы	Баллы по результатам работы
	Обоснование актуальности; корректность постановки цели и задач; соответствие результатов цели и задачам; логичность структуры и изложения, отсутствие противоречий; полнота охвата материала в пределах поставленных задач; аргументированность выводов; обоснованность используемых методов и технологических решений; корректность применения профессиональных знаний и методов; качество графического материала (схемы, рисунки) и его соответствие тексту; обоснованность подбора учебно-научной литературы и информационных источников (кол-во источников – не менее 10); корректность цитирований и соблюдение требований по антиплагиату.	40баллов	
	Качество устного сообщения (доклада и презентации), полнота и профессионализм ответов на вопросы, в т.ч. по замечаниям к тексту курсового проекта.	20 баллов	
	Соблюдение стиля научно-технического текста, грамотность, правильное оформление ссылок на используемую литературу и другие информационные источники, аккуратное форматирование, соответствие требованиям стандарта оформления письменных работ.	20 баллов	
	Соблюдение календарного плана, баллы снижаются при предоставлении КР с задержкой более 5 дней от календарного графика (-5 баллов за неделю).	20 баллов	
Итого		100	

Шкала итоговой оценки:

Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
0-54	55-70	71-85	86-100

Оценочное заключение: _____
(неудовлетворительно/удовлетворительно/хорошо/отлично)

Преподаватель _____

«__» _____20_____г.