МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ АВТОМОБИЛЬНО-ДОРОЖНЫЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (МАДИ)»

ВОЛЖСКИЙ ФИЛИАЛ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ «НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА»

для студентов направления

09.03.01 «Информатика и вычислительная техника»

профиль подготовки

«Автоматизированные системы обработки информации и управления»

Чебоксары 2019 г

Составители:
Изосимова Т.А.

Изосимова Т.А. Методические указания к производственной практики «Научно-исследовательская работа» для студентов направления 09.03.01 «Информатика и вычислительная техника» профиль подготовки «Автоматизированные системы обработки информации и управления». – Чебоксары: Волжский филиал Московского автомобильно-дорожного государственного технического университета (МАДИ), 2019. – 42 с.

Печатается по решению Учебно-методического совета Волжского филиала МАДИ

ОГЛАВЛЕНИЕ

1. ЦЕЛИ И ЗАДАЧИ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Исследовательская работа имеет своей целью ознакомление студентов с реальными условиями, технологиями и методиками коллективного решения научно-технических задач при разработке частной модели угроз безопасности персональных данных при их обработке в ИСПДн.

2. МЕСТО ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ В СТРУКТУРЕ ОПОП

Целью прохождения практики является формирование у обучающихся компетенций в соответствии с требованиями ФГОС и образовательной программы.

Вид практики: производственная.

Задачами прохождения практики являются:

- приобретение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в соответствии с учебным планом и календарным графиком учебного процесса;
- оценка достижения обучающимися планируемых результатов обучения как этапа формирования соответствующих компетенций.

Производственная практика реализуется в рамках вариативной части Блока 2 «Практика. Часть, формируемая участниками образовательных отношений» учебного плана.

Практика базируется на результатах обучения по следующим дисциплинам (модулям), практикам: программирование, операционные системы, объектно-ориентированное программирование, инженерная и компьютерная графика, методы оптимизации теория принятия решений, схемотехника, базы данных, аппаратно-программные комплексы, системное программное обеспечение, моделирование АСОИиУ, Сети ЭВМ и телекоммуникации, защита информации, 3D-программирование, интернет программирование, системы искусственного интеллекта, эксплуатационная практика.

Результаты обучения, достигнутые по итогам прохождения практики являются необходимым условием для успешного обучения по следующими дисциплинам (модулям), практикам:, интерфейсы АСОИиУ, ЭВМ и периферийные устройства, визуальное программирование, теоретические основы автоматизированного управления, информационные технологии на транспорте.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРАКТИКЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате прохождения практики у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать	Перечень планируемых результатов обучения по дисциплине
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает принципы сбора, отбора и обобщения информации. УК-1.2. Умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности. УК-1.3. Имеет практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов.
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Знает необходимые для осуществления профессиональной деятельности правовые нормы. УК-2.2. Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности. УК-2.3. Имеет практический опыт применения нормативной базы и решения задач в области избранных видов профессиональной деятельности.
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1. Знает различные приемы и способы социализации личности и социального взаимодействия. УК-3.2. Умеет строить отношения с окружающими людьми, с коллегами. УК-3.3. Имеет практический опыт участия в командной работе, в социальных

		проектах, распределения ролей в условиях командного взаимодействия.
ПКС-7	Способен руководить рабочей группой технических писателей (специалистов по технической документации в ИТ)	ПКС-7.1. Знает основы управления проектами в сфере информационных технологий, основные форматы электронных документов и их особенности ПКС-7.2. Умеет разрабатывать требования к комплекту технической документации ПКС-7.3. Имеет навыки организации деятельности коллектива разработчиков комплекта технической документации
ПКС-9	Способен обеспечивать информационную безопасность на уровне БД	ПКС-9.1. Знает угрозы безопасности БД и способы их предотвращения; методы анализа и критерии эффективности системы безопасности на уровне БД ПКС-9.2. Умеет разрабатывать мероприятия по обеспечению безопасности на уровне БД ПСК-9.3. Имеет навыки выбора основных средств поддержки информационной безопасности на уровне БД
ПКС-13	Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	ПКС-13.1. Знает средства защиты от несанкционированного доступа операционных систем и СУБД, основные средства криптографии ПКС-13.2. Умеет применять аппаратные, программные и аппаратно-программные средства защиты сетевых устройств от несанкционированного доступа ПКС-13.3. Имеет навыки оценки безопасности и защиты приложений,

		операционных систем от несанкционированного доступа
ПКС-14	Проводить юзабилити-исследование программных продуктов и/или аппаратных средств	ПКС-14.1. Знает методологию планирования и постановки эксперимента; стандарты, регламентирующие требования к эргономике взаимодействия человек-система; методы и приемы обработки эмпирических данных ПКС-14.2. Умеет анализировать данные (качественная и количественная статистика), использовать программы статического анализа ПКС-14.3. Имеет навыки обработки собранных экспериментальных данных пользовательского исследования

4. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Объём (трудоёмкость) практики составляет 4 зачётных единиц (ЗЕ).
Продолжительность практики составляет 144 часов.
Объем контактной работы составляет 5 часов

№ п/п	Этапы проведения практики и их содержание	Трудоемкость (в часах)
1.	Оформление по месту прохождения практики, знакомство с руководителями практики от предприятия и планом–графиком проведения практики.	2
2.	Ознакомление с предприятием, структурами отделов и служб, их взаимодействием. Инструкция по технике безопасности. Анализ деятельности предприятия	6
3.	Изучение нормативно-технической документации предприятия, Анализ используемых информационных систем предприятия	6
4.	Разработка частной модели угроз безопасности персональных данных при их обработке в информационная система персональных данных (ИСПДн).	124
5.	Завершение научно-исследовательской работы (оформление отчета). Сдача зачета по практике.	6

Всего часов	144

5. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Форма аттестации по итогам практики – ***зачет с оценкой.***

Промежуточная аттестация обучающихся в форме зачёта с оценкой проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данному виду практики. Оценка степени достижения обучающимися планируемых результатов обучения по практике проводится преподавателем-руководителем практики методом экспертной оценки. По итогам промежуточной аттестации по практике выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Балл**	**Описание**
Отлично	5	Студент демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности.
Хорошо	4	Студент демонстрирует частичное соответствие знаний, умений, навыков приведенным в таблицах показателей: знания, умения и навыки освоены, но допускаются незначительные ошибки, неточности, затруднения в аналитических операциях, перенос знаний и умений на новые, нестандартные ситуации.
Удовлетворительно	3	Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется недостаточность знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
неудовлетворительно	2	Студент демонстрирует полное отсутствие или явную недостаточность знаний, умений, навыков в соответствии с приведенными показателями.

В рамках выполнения научно-исследовательской работы, студентам необходимо изучить особенности применения автоматизированных информационных систем на предприятии, технических и программных средств защиты персональных данных и разработать частную модель угроз информационной системы персональных данных предприятия, включающую следующие разделы:

1. Описание информационной системы персональных данных предприятия

1.1.Описание условий создания и использования информационной системы персональных данных предприятия

1.2.Описание форм представления информационной системы персональных данных предприятия

1.3.Описание структуры информационной системы персональных данных

предприятия

1.4.Описание характеристик безопасности

2.Описание подхода к моделированию угроз безопасности персональных данных

3.Классификация угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных предприятия

4.Общее описание угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных предприятия

4.1.Угрозы утечки информации по техническим каналам

4.2.Угрозы несанкционированного доступа

5.Модель угроз безопасности персональных данных, обрабатываемых в информационной системе персональных данных предприятия

5.1.Угрозы утечки информации по техническим каналам

5.2.Угрозы несанкционированного доступа к персональных данных, обрабатываемым в информационной системы персональных данных предприятия

5.3.Определение уровня исходной защищенности информационной системы персональных данных предприятия

5.4.Определение вероятности реализации угроз в информационной системе персональных данных предприятия

5.5.Оценка опасности угроз информационной системы персональных данных предприятия

6.Перечень актуальных угроз безопасности персональных данных в информационной системе персональных данных предприятия

6. СТРУКТУРА И СОДЕРЖАНИЕ ОТЧЕТА ПО ПРАКТИКЕ

Формами отчётности по практике являются рабочий дневник по практике и отчёт по практике.

Отчет по производственной практике должен содержать следующую структуру:

1) Титульный лист (Приложение 1).
2) Дневник прохождения практики.
3) Содержание.
4) Выполнение индивидуального практического задания.
5) Список использованных источников.

Форма рабочего дневника по практике приведена в Приложении 2.

Требования к отчету по практике

Отчет по учебной практике должен быть оформлен в соответствии с требованиями ГОСТ 7.32-2001. Страницы текста должны соответствовать формату А4 (210х297мм).

Текст отчета должен быть выполнен на одной стороне листа машинописным способом или с применением печатающих и графических компьютерных устройств.

При использовании персонального компьютера рекомендуется подготовка отчета в MS Word. Параметры документа следующие: межстрочный интервал – 1,5 кегель (размер) – 14, шрифт – Times New Roman. Функция переноса слов обязательна. Текст следует печатать, соблюдая следующие размеры полей: левое – 30 мм, правое – 10 мм, верхнее – 20 мм, нижнее – 20 мм.

Нумерация страниц начинается со страницы, содержащей оглавление работы, и производится арабскими цифрами в правом нижнем углу листа. В приложениях страницы не нумеруются.

Текст основной части работы подразделяется на разделы и подразделы. Каждый раздел следует начинать с новой страницы. Разделы должны иметь порядковую нумерацию единую в пределах всей работы и обозначаться арабскими цифрами и точкой. Введение и заключение не нумеруется. Подразделы нумеруют в пределах каждого раздела. Номер подраздела состоит из номер раздела и подраздела разделенных точкой. В конце номера подраздела также ставится точка. Например: 2.1 (первый подраздел второго раздела).

Разделы и подразделы должны иметь наименования – заголовки, в которых кратно отражается основное содержании текста. Заголовки разделов пишутся симметрично тексту прописными (заглавными) буквами и выделяются жирным шрифтом. Заголовки подразделов пишутся с абзаца строчными буквами, кроме первой – прописной и также выделяются жирным шрифтом. Сокращенное написание слов в заголовках не допускается. Переносы слов в заголовках не допускаются. Точка в конце заголовка не ставят. Если заголовок состоит из двух и более предложений, их разделяют точкой. Подчеркивание заголовков не допускается. Расстояние между заголовками раздела (подраздела) и последующим текстом должно быть одинарному межстрочному интервалу (20 мм), а расстояние меду заголовком подраздела и последней строкой предыдущего текста – 2-м одинарным межстрочным интервалом (15 мм). Иллюстрации, схемы, графики, таблицы, расположенные на отдельных страницах, включаются в общую нумерацию страниц. Документы, бланки, фотоснимки размеров меньше формата А4 должны быть наклеены на стандартные листы или сканированы. Построение диаграмм осуществляется с помощью специального редактора Word.

В тексте не должно быть рисунков и таблиц без ссылок на них:

Рисунки располагаются в тексте сразу после ссылок.

Рисунки должны иметь поясняющую надпись – название рисунка, которая помещается под ним.

Рисунки обозначаются словом «Рисунок».

Точка в конце названия не ставится.

Рисунки следует нумеровать последовательно арабскими цифрами в сквозном порядке в пределах всего отчета.

При повторной ссылке на рисунок пишут сокращено слово «смотри», например: см. рис.2.

Цифровой материал целесообразно оформлять в виде таблиц. Каждая таблица должна иметь заголовок, который должен быть кратким и отражать содержимое таблицы. Над названием справа пишется слово «Таблица» с порядковым номером арабскими цифрами в сквозном порядке в пределах всего отчета. Тематический заголовок пишут строчными буквами, кроме первой прописной. В конце заголовка точку не ставят. Таблицу следует помещать после первого упоминания о ней в тексте и размещать так, чтобы ее можно было читать без поворота работы или же с поворотом по часовой стрелке. Таблицу с большим количеством строк допускается переносить на другую страницу. При переносе таблицы, на следующей странице повторяют ее шапку и над ней помещается надпись «Продолжение табл.» с указанием номера. Если шапка таблицы громоздкая, то вместо нее с перенесенной части в отдельной строке помещают номер граф. При повторной ссылке на таблицу пишут сокращенно словосочетание «смотри таблицу», например: см. табл. 4.

Приложение оформляется как продолжение отчета, располагается в порядке появления ссылок в тексте. Каждое приложение должно начинаться с новой страницы и иметь содержательный заголовок, напечатанный прописными буквами. В правом верхнем углу над заголовком прописными буквами печатается слово «ПРИЛОЖЕНИЕ». Нумерация разделов, пунктов, таблиц в каждом приложении своя.

7. СТРУКТУРА ЧАСТНОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДн

Пример описания информационной системы персональных данных организации ИСПДн «Кадры»

Организация: ЗАО «Солнышко».
Директор: Иванов Иван Иванович.
Заместитель директора: Петрова Тамара Васильевна.
Начальник отдела кадров: Южина Мария Ивановна.
Сотрудники отдела кадров: Сидорова Александра Павловна,
Копылова Юлия Фёдоровна.

Описание ИСПДн:

Состав:

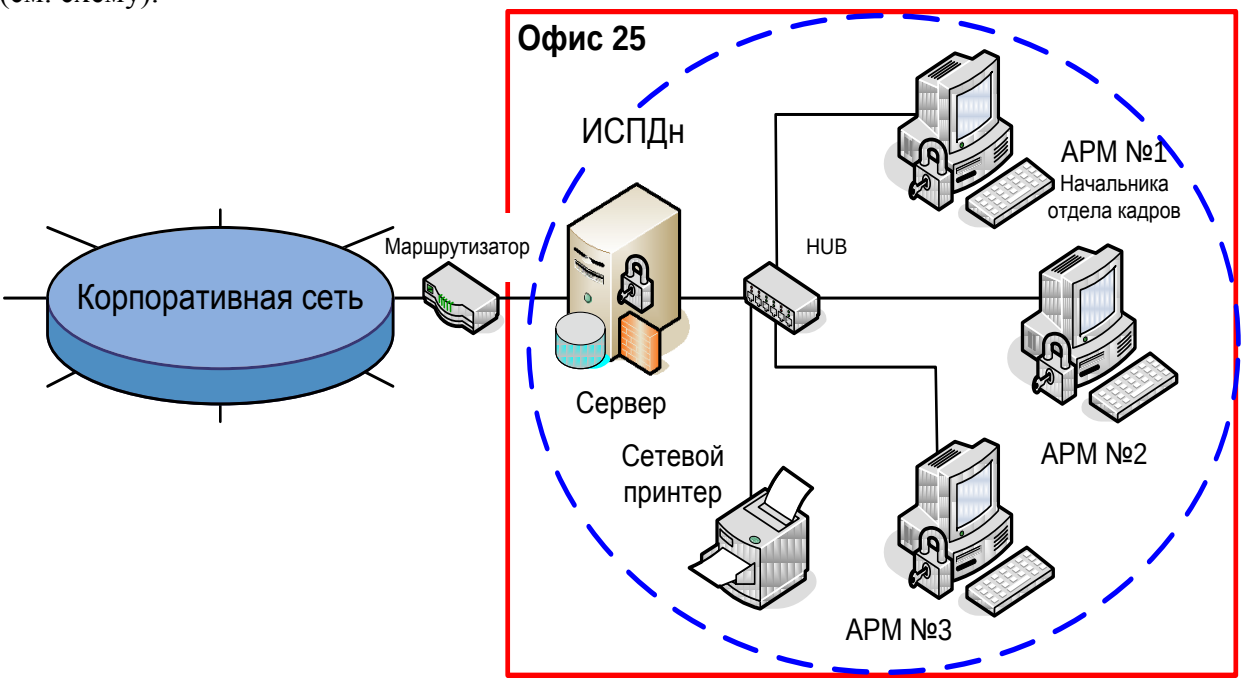
- Персональные данные сотрудников организации:
- фамилия, имя, отчество
- дата и место рождения
- пол
- сведения об образовании
- сведения о предыдущем месте работы
- семейное положение (ФИО жены/мужа, ФИО и даты рождения детей)
- адреса регистрации и фактического проживания
- номера контактных телефонов
- индивидуальный номер налогоплательщика
- номер страхового свидетельства пенсионного страхования

– номер полиса обязательного медицинского страхования
– данные водительского удостоверения

В информационной системе одновременно обрабатываются данные 777 субъектов персональных данных (сотрудников) в пределах Организации.

1. Три автоматизированных рабочих места (АРМ) пользователей, сетевой принтер, сервер, коммутационное оборудование.

Топология: АРМ и сервер составляют сегмент корпоративной вычислительной сети (см. схему).



Корпоративная сеть Организации не имеет подключения к сетям связи общего пользования и сетям международного информационного обмена.

В состав каждого АРМ входят два жёстких диска, на первом установлена операционная система, прикладное программное обеспечение и общедоступная справочная информация, на втором - информация, составляющая персональные данные сотрудников Организации.

Комплект АРМ №1-3 (см. схему): Системный блок № XXXXXXX01-03, Монитор Samsung N710 – серийный номер YYYYYYY01-03, клавиатура Genius серийный номер ZZZZZZZZ01-03, графический манипулятор (мышь) Genius серийный номер WWWW01-03,

В состав сервера входят три жестких диска, на первом установлена операционная система, прикладное программное обеспечение, второй и третий объединены в RAID массив, в котором хранится информация, составляющая персональные данные сотрудников Организации.

Комплект сервера: Системный блок № XXXXXXX04, Монитор Samsung N710 – серийный номер YYYYYYY04, клавиатура Genius серийный номер ZZZZZZZZ04, графический манипулятор Genius серийный номер WWWW04.

Сервер и коммуникационное оборудование установлены в типовой стойке.

Сетевой принтер HP LaserJet P2015 серийный номер SSSSSSSSS.

2. Технология обработки персональных данных:

Обработка персональных данных сотрудников включает весь перечень действий.

К работе на АРМ допущены сотрудники отдела кадров и заместитель директора.

Полный доступ ко всей информации на АРМ и сервере имеют заместитель директора

и начальник отдела кадров.

Сотрудники отдела кадров имеют полный доступ только к каталогу «Личные дела», размещённой на диске №2 своего АРМ, и только на чтение информации из каталога «Личные дела» на сервере.

Системный администратор сегмента сети не имеет доступа к информации, составляющей персональные данные. Имеет права на инсталляцию, настройку программного обеспечения, программных (программно-аппаратных) средств защиты сервера и АРМ № 1-3.

Режим работы - одновременный.

Расположение: Отдельный кабинет по адресу: РФ, г. Глупов, ул. Кривая, дом 6, офис 25. Помещение офиса оборудовано охранной сигнализацией и в нерабочее время сдается под охрану. Доступ в помещение ограничен распорядительными актами Организации и автоматизированной системой контроля и управления доступа.

УТВЕРЖДАЮ

_____

(должность руководителя организации)

_____

(подпись)

«_____» _____ 201 ____г.

Частная модель угроз

безопасности персональных данных
при их обработке в ИСПДн

_____

(наименование ИСПДн)

СОГЛАСОВАНО

_____

«____» _____ 201___ г.

СОГЛАСОВАНО

_____

«____» _____ 201___ г.

20___ г.

Содержание

Сокращения, условные обозначения

Термины и определения

Введение.

Современная система обеспечения информационной безопасности

должна строиться на основе комплексирования разнообразных мер защиты и должна опираться на современные методы прогнозирования, анализа и моделирования возможных угроз безопасности информации и последствий их реализации.

Результаты моделирования предназначены для выбора адекватных оптимальных методов парирования угроз.

На стадии моделирования проведено изучение и анализ существующей обстановки и выявлены актуальные угрозы безопасности ПДн в составе ИСПДн_____

Модель угроз построена в соответствии с

1. Описание ИСПДн

1.1. Описание условий создания и использования ПДн

1.2. Описание форм представления ПДн

1.3. Описание структуры ИСПДн

1.4. Описание характеристик безопасности

2. Описание подхода к моделированию угроз безопасности ПДн.

Модель угроз безопасности ПДн в составе ИСПДн разработана на основе методических документов ФСТЭК:

На основе «Базовой модели угроз безопасности ПДн при их обработке в ИСПДн» проведена классификация угроз безопасности ПДн в составе ИСПДн и составлен перечень угроз безопасности ПДн в составе ИСПДн.

На основе составленного перечня угроз безопасности ПДн в составе ИСПДн с помощью «Методики определения актуальных угроз безопасности ПДн при их обработке в ИСПДн» построена модель угроз безопасности ПДн в составе ИСПДн и выявлены актуальные угрозы.

3. Классификация угроз безопасности персональных данных в ИСПДн

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угроз.

К характеристикам ИСПДн, обуславливающим возникновение УБПДн, можно отнести:

ИСПДн представляет собой совокупность информационных и программно-аппаратных элементов и их особенностей как объектов обеспечения безопасности.

Основными элементами ИСПДн являются:

Основными **элементами канала реализации** УБПДн являются:

Носители ПДн могут содержать информацию, представленную в следующих видах:

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн угрозы классифицируются в соответствии со следующими признаками:

Реализация одной из УБПДн перечисленных классов или их совокупности может привести к следующим **типам последствий** для субъектов ПДн:

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн и описываются следующим образом:

Угрозы, связанные с НСД, представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

4. Общее описание угроз безопасности ПДн, обрабатываемых в ИСПДн

При обработке ПДн в ИСПДн возможна реализация следующих видов УБПДн:

4.1 Угрозы утечки информации по техническим каналам.

Основными элементами угроз утечки информации по техническим каналам являются:

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

Возникновение угроз утечки акустической (речевой) информации, содержащаяся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера. Основную опасность представляют угрозы утечки из-за наличия электромагнитных излучений монитора.

4.2 Угрозы несанкционированного доступа.

Угрозы НСД в ИСПДн с применением программных и программно-аппаратных средств реализуются при осуществлении несанкционированного, в том числе случайного доступа, в результате которого осуществляется нарушение конфиденциальности (копирования, несанкционированного распространения), целостности (уничтожения, изменения) и доступности (блокирования) ПДн, и включают в себя:

5 Модель угроз безопасности ПДн, обрабатываемых в ИСПДн

При обработке ПДн в ИСПДн, возможна реализация следующих видов УБПДн:

_____

_____

_____

5.1 Угрозы утечки информации по техническим каналам.

При обработке ПДн в ИСПДн возможно возникновение УБПДн за счет реализации следующих технических каналов утечки информации:

_____

_____

_____

5.1.1Угрозы утечки акустической (речевой) информации.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, обусловлено наличием функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

Утечка акустической (речевой) информации может быть осуществлена:

_____

_____

_____

В ИСПДн не реализованы функции голосового ввода ПДн в ИСПДн. Акустические средства воспроизведения ПДн в ИСПДн не предусмотрены.

Рассмотрение угроз утечки акустической (речевой) информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

5.1.2 Угрозы утечки видовой информации.

Угрозы утечки видовой информации реализуются за счет просмотра ПДн с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн.

Необходимым условием осуществления просмотра (регистрации) ПДн является наличие прямой видимости между средством наблюдения и носителем ПДн.

Утечка видовой информации может быть осуществлена:

В ИСПДн отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от них, соответственно отсутствует возможность непосредственного наблюдения посторонними лицами ПДн.

Рассмотрение угроз утечки видовой информации не целесообразно в связи с отсутствием предпосылок возникновения угроз.

5.1.3 Угрозы утечки информации по каналам ПЭМИН.

Возникновение угрозы ПДн по каналам ПЭМИН возможно за счет перехвата техническими средствами побочных информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПДн техническими средствами ИСПДн.

Рассмотрение угроз безопасности ПДн, связанных с перехватом ПЭМИН в ИСПДн, избыточно, так как носители ПДн (технические средства ИСПДн, создающие физические поля, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин) находятся в пределах контролируемой зоны.

Утечка ПДн по каналам ПЭМИН – маловероятна из-за несоответствия стоимости средств съема информации и полученной в результате регистрации ПЭМИН информации, а защита ПДн от данного вида угроз – экономически нецелесообразна.

5.2 Угрозы НСД к ПДн, обрабатываемым в ИСПДн.

Угрозы НСД связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн. Кроме этого, источниками угроз НСД к информации в ИСПДн могут быть аппаратные закладки и отчуждаемые носители вредоносных программ.

В ИСПДн возможны:

5.2.1. Общая характеристика источников угроз НСД.

Источниками угроз НСД в ИСПДн могут быть:

5.2.1.1. Нарушитель.

Внутренние потенциальные нарушители подразделяются на **восемь категорий** в зависимости от способа доступа и полномочий доступа к ПДн (Таблица 1).

Таблица 1 – Категории нарушителей

Категория нарушителя	**Способ доступа и полномочия**

5.2.1.2. Носитель вредоносной программы.

Носителем вредоносной программы может быть аппаратный элемент компьютера или программный контейнер. Если вредоносная программа не ассоциируется с какой-либо прикладной программой, то в качестве ее носителя рассматриваются:

Если вредоносная программа ассоциируется с какой-либо прикладной программой, с файлами, имеющими определенные расширения или иные атрибуты, с сообщениями, передаваемыми по сети, то ее носителями являются:

1. пакеты передаваемых по компьютерной сети сообщений;

2. файлы (текстовые, графические, исполняемые и т.д.).

5.2.1.3. Аппаратная закладка.

В ИСПДн имеется опасность применения аппаратных средств, предназначенных для регистрации вводимой с клавиатуры информации, например:

В ИСПДн отсутствует возможность неконтролируемого пребывания физических лиц в служебных помещениях или в непосредственной близости от них, соответственно отсутствует возможность установки аппаратных закладок посторонними лицами.

Существование данного источника угроз маловероятно также из-за несоответствия стоимости аппаратных закладок, сложности их скрытой установки и полученной в результате информации.

5.2.2. Общая характеристика уязвимостей ИСПДн.

Уязвимость ИСПДн – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данным.

Причины возникновения уязвимостей:

К основным группам уязвимостей ИСПДн, относятся:

5.2.2.1. Характеристика уязвимостей системного ПО.

Уязвимости системного программного обеспечения необходимо рассматривать с привязкой к архитектуре построения вычислительных систем. При этом возможны уязвимости:

Уязвимости в микропрограммах и в средствах операционной системы, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др.

5.2.2.2. Характеристика уязвимостей прикладного ПО.

К прикладному программному обеспечению относятся прикладные программы общего пользования и специальные прикладные программы.

Прикладные программы общего пользования – это

Специальные прикладные программы – это

Уязвимости прикладного программного обеспечения могут представлять собой:

5.2.3. Характеристика угроз непосредственного доступа в операционную среду ИСПДн.

Угрозы доступа (проникновения) в операционную среду компьютера и несанкционированного доступа к ПДн связаны с доступом:

Эти угрозы могут быть реализованы в случае получения физического доступа к ИСПДн или, по крайней мере, к средствам ввода информации в ИСПДн:

5.2.3.1. Угрозы, реализуемые в ходе загрузки операционной системы

5.2.3.2. Угрозы, реализуемые после загрузки операционной среды независимо от того, какая прикладная программа запускается пользователем

5.2.3.3. Угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем, или фактом запуска любой из прикладных программ. Большая часть таких угроз – это угрозы внедрения вредоносных программ.

5.2.4. Общая характеристика УБПДн, реализуемых с использованием протоколов межсетевого взаимодействия.

Классификация угроз, реализуемых по сети, приведена в Таблице 2. В ее основу положено семь первичных признаков классификации.

Таблица 2 – Классификация угроз, реализуемых по сети

№ п/п	Признак классификации	Тип угрозы	Описание

С учетом проведенной классификации можно выделить _____ угроз, реализуемых с использованием протоколов межсетевого взаимодействия:

5.2.4.1. Анализ сетевого трафика.

5.2.4.2. Сканирование сети.

5.2.4.3. Угроза выявления пароля.

5.2.4.4. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.

5.2.4.5. Навязывание ложного маршрута сети.

5.2.4.6. Внедрение ложного объекта сети.

5.2.4.7. Отказ в обслуживании.

5.2.4.8. Удаленный запуск приложений.

5.2.5. Общая характеристика угроз программно-математических воздействий.

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

Вредоносные программы могут быть внесены (внедрены) как преднамеренно, так и случайно в программное обеспечение, используемое в ИС, в процессе его разработки, сопровождения, модификации и настройки. Кроме этого, вредоносные программы могут быть внесены в процессе эксплуатации ИС с внешних носителей информации или посредством сетевого взаимодействия как в результате НСД, так и случайно пользователями ИС.

Основными видами вредоносных программ являются:

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

5.2.6. Общая характеристика нетрадиционных информационных каналов.

Нетрадиционный информационный канал - это …….

Для формирования нетрадиционных каналов могут использоваться методы:

Методы компьютерной стеганографии предназначены для скрытия факта передачи сообщения путем встраивания скрываемой информации во внешне безобидные данные (текстовые, графические, аудио- или видеофайлы) и включают в себя **две группы методов**, основанных:

Нетрадиционные информационные каналы могут быть сформированы на различных уровнях функционирования ИСПДн:

_____

_____

_____

5.2.7. Общая характеристика результатов несанкционированного или случайного доступа.

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

5.2.7.1. Нарушению конфиденциальности (копирование, неправомерное распространение), которое может быть осуществлено в случае утечки информации за счет:

_____

_____

_____

5.2.7.2. Нарушению целостности (уничтожение, изменение) за счет воздействия (модификации) на программы и данные пользователя, а также технологическую (системную) информацию, включающую:

_____

_____

_____

Нарушение целостности информации в ИСПДн может также быть вызвано внедрением в нее вредоносной программы программно-аппаратной закладки или воздействием на систему защиты информации или ее элементы.

Кроме этого, в ИСПДн возможно воздействие на технологическую сетевую информацию, которая может обеспечивать функционирование различных средств управления вычислительной сетью:

_____

_____

_____

5.2.7.3. Нарушению доступности (блокирование) путем формирования (модификации) исходных данных, которые при обработке вызывают неправильное функционирование, отказы аппаратуры или захват (загрузку) вычислительных ресурсов системы, которые необходимы для выполнения программ и работы аппаратуры.

Указанные действия могут привести к нарушению или отказу функционирования практически любых технических средств ИСПДн:

5.3 Определение уровня исходной защищенности ИСПДн

Под уровнем исходной защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1).

Таблица 3 – Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению			
2. По наличию соединения с сетями общего пользования:			
3. По встроенным (легальным) операциям с записями баз персональных данных:			
4. По разграничению доступа к персональным данным:			
5. По наличию соединений с другими базами ПДн иных ИСПДн:			
6. По уровню обобщения (обезличивания) персональных данных:			
7. По объему персональных данных, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			

В соответствии с Таблицей 3, _____ % характеристик ИСПДн соответствуют уровню не ниже "_____", следовательно Y_1= _____ .

ИСПДн имеет _____ степень исходной защищенности.

5.4. Определение вероятности реализации угроз в ИСПДн

Под вероятностью реализации угрозы поднимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализации конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вероятность (Y_2) определяется по 4 вербальным градациям этого показателя:

Таблица 4 – Определение вероятности реализации угроз в ИСПДн

Градация	Описание	Вероятность (Y2)

Оценка вероятности реализации угрозы безопасности различными категориями нарушителей приведена в Таблице 5.

Таблица 5 – Оценка вероятности реализации угрозы безопасности различными категориями нарушителей

Угроза безопасности ПДн	Вероятность реализации угрозы нарушителем категории Кn

По итогам оценки уровня исходной защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы (Таблица 6). Коэффициент реализуемости угрозы рассчитывается по формуле: $Y=(Y_1+Y_2)/20$.

Таблица 6 – Определение коэффициента реализуемости угрозы

Угроза безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации угрозы

5.5. Оценка опасности угроз ИСПДн

Оценка опасности производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет 3 значения:

5.5.1. **низкая опасность** – ……;

5.5.2. **средняя опасность** – ……;

5.5.3. **высокая опасность** – ……..

Оценка опасности приведена в Таблице 7.

Таблица 7 – Оценка опасности

Угроза безопасности ПДн	**Опасность угроз**

6. Перечень актуальных УБПДн в ИСПДн

Правила, отнесения угроз к актуальным приведены в Таблице 8.

Таблица 8 – Правила, отнесения угроз к актуальным

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

В соответствии с правилами отнесения угроз безопасности к актуальным, для ИСПДн существуют следующие актуальные угрозы (Таблица 9).

Таблица 9 – Актуальные угрозы

Угроза безопасности ПДн	**Опасность угроз**

Таким образом, актуальными угрозами безопасности ПДн в ИСПДн являются:

_____

_____

_____

_____

Угроза	Y_1	Частота реализации	Y_2	Y	Реализуемость угрозы	Показатель опасности	Актуальность
угроза модификации базовой системы ввода/вывода (BIOS),							
угроза перехвата управления загрузкой							
угроза НСД с применением стандартных функций операционной системы							
угроза НСД с помощью прикладной программы							
угроза НСД с применением специально созданных для этого программ							
угроза НСД при передаче информации по внешним каналам							
угроза утечки информации при удаленном доступе к информационным ресурсам							
угроза утечки информации с использованием копирования ее на съемные носители;							
угроза утечки данных посредством печати информации, содержащей персональные данные;							
угроза утечки информации за счет ее несанкционированной передачи по каналам связи							
угроза внедрения вредоносных программ с использованием съемных носителей							
угроза «Анализа сетевого трафика»							

угроза сканирования направленного на выявление открытых портов и служб, открытых соединений и др.							
угроза обхода системы идентификации и аутентификации сообщений							
угроза обхода системы идентификации и аутентификации сетевых объектов							
угроза внедрения ложного объекта сети							
угроза навязывания ложного маршрута							
угроза перехвата и взлома паролей							
угроза подбора паролей доступа							
угроза типа «Отказ в обслуживании»							
угроза внедрения троянских программ							
угроза атаки типа «переполнение буфера»;							
угроза удаленного запуска приложений с использованием средств удаленного управления							
угроза внедрения вредоносных программ через почтовые сообщения							
угроза внедрения вредоносных программ через обмен и загрузку файлов							
угроза заражения сетевыми червями, использующими уязвимости сетевого ПО							

Заключение.

В настоящем документе проведена классификация УБПДн в ИСПДн, дано общее описание УБПДн и построена Модель угроз. В соответствии с требованиями методических документов ФСТЭК России, выявлены актуальные угрозы безопасности ПДн в ИСПДн, на основе которых в дальнейшем должны быть разработаны Требования по обеспечению безопасности ПДн в ИСПДн.

Построенная Модель угроз безопасности ПДн в ИСПДн применима к существующему состоянию ИСПДн при условии соблюдения основных (базовых) исходных данных:

- технические средства ИСПДн находятся в пределах контролируемой зоны;
- ИСПДн физически отделена от сетей общего пользования;
- отсутствует возможность неконтролируемого пребывания посторонних лиц в служебных помещениях ИСПДн и др.

В случае несоблюдения и/или изменения вышеуказанных условий Модель угроз безопасности ПДн в ИСПДн должна быть пересмотрена.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

а) основная литература:

1. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками : учебное пособие / П.Н. Девянин. — 2-е изд., испр. и доп. — Москва : Горячая линия-Телеком, 2017. — 338 с. — ISBN 978-5-9912-0328-9. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/111049
2. Жук А.П., Жук Е.П., Лепешкин О.М. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин. - 2-е изд. - М. : РИОР : ИНФРА-М, 2018. - 392 с. - Режим доступа: http://znanium.com/catalog/product/937469
3. Рябко, Б.Я. Криптографические методы защиты информации : учебное пособие / Б.Я. Рябко, А.Н. Фионов. — 2-е изд., стер. — Москва : Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0286-2. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/111097
4. Рябко, Б.Я. Основы современной криптографии и стеганографии : монография / Б.Я. Рябко, А.Н. Фионов. — 2-е изд. — Москва : Горячая линия-Телеком, 2016. — 232 с. — ISBN 978-5-9912-0350-0. — Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. — URL: https://e.lanbook.com/book/111098
5. Шаньгин В.Ф Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. —Режим доступа: http://znanium.com/catalog/product/546679

б) дополнительная литература:

1. Гришина Н.В. Организация комплексной системы защиты информации. - М.: Гелиос АРВ, 2007. - 256с.
2. Куприянов А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, В.А. Сахаров, В.А. Шевцов. – 2-е изд., стер. – М.: Издательский центр « Академия», 2007. – 256с.
3. Петраков, А. В. Основы практической защиты информации [Текст] : учеб. пособие / А. В. Петраков. - 4-е изд., доп. - М. : СОЛОН-ПРЕСС, 2005. - 384 с
4. Филин, С. А. Информационная безопасность: Учебное пособие. [Текст] / С. А. Филин. - [Б. м.] : Издательство "Альфа-Пресс", 2006. - 412 с
5. Хорев, П. Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений. [Текст] / П. Б. Хорев. - М. : Издательский центр "Академия", 2005. - 256 с.
6. Аверченков, В.И. Автоматизация проектирования комплексных систем защиты информации: монография / В.И. Аверченков, М.Ю. Рытов, О.М. Голембиовская. – 2-е изд. – Москва: ФЛИНТА, 2017. – 145 с. – ISBN 978-5-9765-2945-8. – Текст: электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/92913

7. Аверченков, В.И. Криптографические методы защиты информации : учебное пособие / В.И. Аверченков, М.Ю. Рытов, С.А. Шпичак. – 2-е изд. – Москва : ФЛИНТА, 2017. – 215 с. – ISBN 978-5-9765-2947-2. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/92914
8. Бекетнова, Ю.М. Международные основы и стандарты информационной безопасности финансово-экономических систем: учебное пособие / Ю.М. Бекетнова, Г.О. Крылов, С.Л. Ларионова. – Москва: Прометей, 2018. – 174 с. – ISBN 978-5-907003-27-9. – Текст: электронный // Электронно-библиотечная система «Лань»: [сайт]. – URL: https://e.lanbook.com/book/121494
9. Бондаренко, И.С. Методы и средства защиты информации: учебное пособие / И.С. Бондаренко, Ю.В. Демчишин. – Москва: МИСИС, 2018. – 32 с. – Текст: электронный // Электронно-библиотечная система «Лань»: [сайт]. – URL: https://e.lanbook.com/book/115269

в) ресурсы сети «Интернет», программное обеспечение и информационно-справочные системы:

1. http://www.vf.madi.ru/moodle - Электронная информационно-образовательная среда ВФ МАДИ
2. https://e.lanbook.com - Электронно-библиотечная система «Лань»
3. https://znanium.com - Электронно-библиотечная система « Znanium.com»
4. https://www.intuit.ru - Бесплатное дистанционное обучение в Национальном Открытом Университете «ИНТУИТ»

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ АВТОМОБИЛЬНО-ДОРОЖНЫЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (МАДИ)»

ВОЛЖСКИЙ ФИЛИАЛ

Факультет _____

Кафедра гуманитарных и естественнонаучных дисциплин

ОТЧЕТ

по производственной практике

(Научно-исследовательская работа)

студент:

_____ курса, группы_____

_____(Ф.И.О. студента) _____

(подпись)

Руководитель практики от предприятия:

_____(должность, название организации)

_____(Ф.И.О. руководителя) _____

(подпись)

Руководитель практики от ВФ МАДИ:

к.т.н., доцент

Изосимова Т.А. _____

(подпись)

Сдан на проверку «__» _____20_ г.

Допущен к защите «__» _____20_ г.

Оценка_____ «__» _____20_ г.

Чебоксары 20__

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ АВТОМОБИЛЬНО-ДОРОЖНЫЙ
ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (МАДИ)»
ВОЛЖСКИЙ ФИЛИАЛ

РАБОЧИЙ ДНЕВНИК
по практике

_____

(Ф.И.О. студента полностью)

студента _____курса факультета _____

специальность/ направление _____

_____

группа _____ проходившего _____

(вид практики)

_____

(название предприятия / организации)

с «____»_____20___г. по «____»_____20___ г.

Чебоксары 20___ г.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРАКТИКУ

_____

_____

_____

_____

_____

Вопросы для изучения _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Содержание ежедневных записей

Дата	Краткое описание выполненных работ	Замечания и предложения проверяющих дневник, подпись и дата

Отзыв о прохождении практики

Студент _____
(Ф.И.О. студента полностью)
факультета_____ Волжского филиала МАДИ группы _____, _____ курса, в период с «____»_____ 20___г. по «____»_____ 20___г.

проходил практику в _____

_____
(наименование организации, предприятия, учреждения)

За время практики работал на должности:

_____ с «____»_____20___г. по «____»_____20___г.

Характеристика производственной деятельности студента:

_____

_____

_____

_____

_____

Считаем, что работа студента _____
(Ф.И.О. студента полностью)

за период практики заслуживает _____ оценки

Особые замечания и предложения _____

_____

_____

Руководитель практики от организации_____ _____
(подпись) (Ф.И.О.)

Руководитель практики от Волжского филиала МАДИ _____ _____
(подпись) (Ф.И.О.)

М.П. «_____» _____ 20___г.