# МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования

# МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ

──────────────────────────────────────

Факультет СиСС

Кафедра Технологии электронного обмена данными (ТЭОД)

# Практическая работа №1-2

по дисциплине «Обеспечение доверия и безопасности в инфокоммуникационных сетях»

на тему:

# «Основы проектирования системы защиты объектов информатизации»

Выполнил: студ. гр. БСС2202

Вечерский В.С. Проверила: Владыченская В.А.

(Осенний семестр) Москва 2024

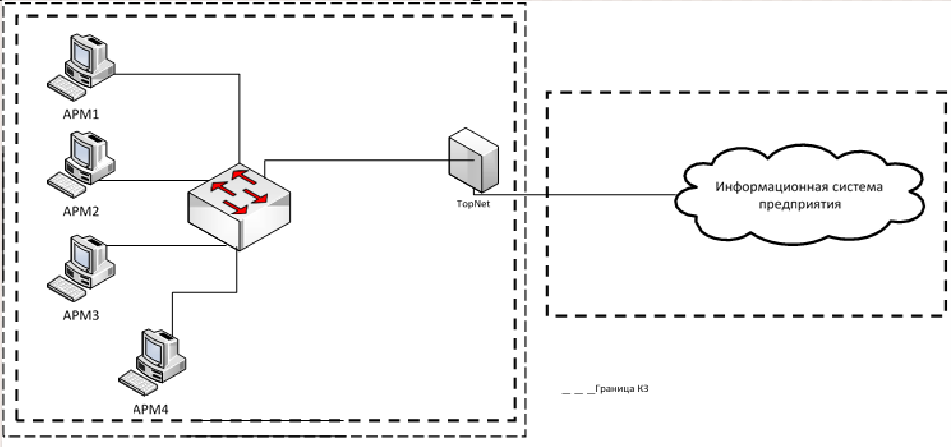
# Краткое описание магазина «DNS»

DNS — это российская сеть магазинов, специализирующаяся на продаже компьютерной техники, электроники и бытовой техники. Основанная в 1998 году, компания быстро завоевала популярность благодаря широкому ассортименту товаров, включая компьютеры, ноутбуки, смартфоны, аксессуары и бытовую технику от различных производителей. Магазины DNS предлагают как розничную, так и онлайн-продажу, а также услуги по сборке и настройке техники.

Сеть ориентирована на широкий круг покупателей, предлагая товары как для частных клиентов, так и для бизнеса. DNS также активно проводит акции и распродажи, что делает её конкурентоспособной на рынке.

Недавно компания открыла новое отделение в городе N, ее ресурсы не велики, но в салоне присутствует 4 АРМ для сотрудников, на которых установлен уникальные программы. Все АРМ подключены к коммутатору, он же в свою очередь к маршрутизатору от компании «TopNet», через который заказы передаются на кухню, где уже идет сборка заказа.

# Сведения об информационной системе

****

**Модель потенциального нарушителя по требованиям ФСТЭК России**

ВНЕШНИЙ

ВНУТРЕННИЙ

НАРУШИТЕЛЬ

Внешние субъекты (физические лица)

Недобросовестные партнеры

Конкуренты (конкурирующие организации)

Криминальные структуры

Разведывательные службы государств

Подрядные организации, осуществляющие поставку, сопровождение и ремонт компонентов ИС

Разработчики ИС

Администратор безопасности ИС

Системный администратор ИС

Администратор безопасности сегмента ИС

Удаленные пользователи ИС

Пользователи ИС

Сотрудники Учреждения, не являющиеся пользователями защищаемой ИС

# Перечень возможностей потенциальных внешних нарушителей

|  |  |  |
| --- | --- | --- |
| **№** | **Возможности внешнего нарушителя** | **ИС**  **«DNS»** |
| **1.** | возможность осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений | + |
| **2.** | возможность осуществлять несанкционированный  доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или)  сетям международного информационного обмена |  |
| **3.** | возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок | + |

|  |  |  |
| --- | --- | --- |
| **4.** | возможность осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИС,  которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за  пределами контролируемой зоны | + |
| **5.** | возможность осуществлять несанкционированный доступ через информационные системы взаимодействующих  ведомств, организаций и учреждений при их подключении к ИС | + |

**Перечень возможностей внутреннего нарушителя**

|  |  |  |
| --- | --- | --- |
| **№** | **Возможности (в т.ч. владение информацией) внутреннего нарушителя** | **ИС**  **« DNS»** |
| **1.** | иметь доступ к фрагментам информации, содержащей защищаемую информацию и распространяющейся по внутренним каналам связи ИС | + |
| **2.** | располагать фрагментами информации о топологии ИС (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах | + |
| **3.** | располагать именами и вести выявление паролей зарегистрированных пользователей | + |
| **4.** | изменять конфигурацию технических средств ИС, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИС | + |
| **5.** | знает, по меньшей мере, одно легальное имя доступа | + |
| **6.** | обладает всеми необходимыми атрибутами (например,  паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации | + |
| **7** | располагает конфиденциальными данными, к которым имеет доступ | + |

|  |  |  |
| --- | --- | --- |
| **8** | располагает информацией о топологии ИС на базе локальной и (или) распределенной информационной системы, через  которую осуществляется доступ, и о составе технических средств ИС |  |
| **9** | имеет возможность прямого (физического) доступа к фрагментам технических средств ИС | + |
| **10** | обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИС |  |
| **11** | обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИС | + |
| **12.** | имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИС |  |
| **13.** | имеет доступ ко всем техническим средствам сегмента (фрагмента) ИС | + |
| **14.** | обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИС |  |
| **15.** | обладает полной информацией о системном и прикладном программном обеспечении ИС |  |
| **16.** | обладает полной информацией о технических средствах и конфигурации ИС |  |
| **17.** | имеет доступ ко всем техническим средствам обработки информации и данным ИС |  |
| **18.** | обладает правами конфигурирования и административной настройки технических средств ИС |  |

# Определение уровня исходной защищенности Y1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **п/п** | **Технические и эксплуатационные характеристики ИСПДн** | **Высок ая** | **Средня я** | **Низкая** |
| **1.По территориальному размещению** | | | | |
| **1.1.** | распределённая ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; |  |  |  |
| **1.2.** | городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка); |  |  |  |
| **1.3.** | корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации; |  |  |  |
| **1.4.** | локальная (кампусная) ИСПДн, развернутая в пределах нескольких  близко расположенных зданий; |  | V |  |
| **1.5.** | локальная ИСПДн, развернутая в пределах одного здания. |  |  |  |
| **2.По наличию соединения с сетями общего пользования:** | | | | |
| **2.1.** | ИСПДн, имеющая многоточечный выход в сеть общего пользования; |  |  |  |
| **2.2.** | ИСПДн, имеющая одноточечный выход в сеть общего пользования; |  |  |  |
| **2.3.** | ИСПДн, физически отделенная от сети общего пользования. | V |  |  |
| **3.По встроенным (легальным) операциям с записями баз персональных данных:** | | | | |
| **3.1.** | чтение, поиск; |  |  |  |
| **3.2.** | запись, удаление, сортировка; |  | V |  |
| **3.3.** | модификация, передача. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **4. По разграничению доступа к персональным данным:** | | | | |
| **4.1.** | ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн; |  | V |  |
| **4.2.** | ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн; |  |  |  |
| **4.3.** | ИСПДн с открытым доступом. |  |  |  |
| **5.По наличию соединений с другими базами ПДн иных ИСПДн** | | | | |
| **5.1.** | интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является  владельцем всех используемых баз ПДн); |  |  |  |
| **5.2.** | ИСПДн, в которой используется одна база ПДн, принадлежащая организации- владельцу данной ИСПДн. | V |  |  |
| **6. По уровню (обезличивания) ПДн:** | | | | |
| **6.1.** | ИСПДн в которой предоставляемые пользователю данные являются  обезличенными (на уровне организации, отрасли, области, региона и т.д.); |  |  |  |
| **6.2.** | ИСПДн, в которой данные  обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в  организации; |  |  |  |
| **6.3.** | ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует  информация, позволяющая идентифицировать субъекта ПДн). |  |  | V |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **7.По объему ПДн, которые предоставляются сторонним пользователям без обработки:** | | | | |
| **7.1.** | ИСПДн, предоставляющая всю БД с ПДн; |  |  | V |
| **7.2.** | ИСПДн, предоставляющая часть ПДн; |  |  |  |
| **7.3.** | ИСПДн, не предоставляющие никакой информации. |  |  |  |
| **7.4.** | Количество баллов по уровням | 2 | 3 | 2 |
| **7.5.** | Уровень исходной защищенности ИСПДн | средний | | |
| **7.6.** | Коэффициент защищенности ИСПДн (Y1) | 5 | | |

**Оценка вероятности и возможности реализации угрозы безопасности**

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование УБИ** | **Угрозы безопасности ПДн** | **Вероятность реализации угрозы Y2** | **Возможность реализации угрозы Y** |
|  | | | |
| **170** | Угроза «кражи» учётной записи доступа к сетевым сервисам | Маловероятно | Низкая |
| **158** | Угроза утраты носителей информации | Средняя | Средняя |
| **141** | Угроза преодоления физической защиты | Средняя | Средняя |
| **20** | Угроза загрузки нештатной операционной системы | Низкая | Средняя |
| **88** | Угроза  несанкционированного | Средняя | Средняя |

|  |  |  |  |
| --- | --- | --- | --- |
|  | изменения  аутентификационной информации |  |  |
| **93** | Угроза  несанкционированного редактирования реестра | Маловероятно | Низкая |
| **212** | Угроза нарушения работы  информационной  системы, вызванного обновлением  используемого в ней программного  обеспечения | Маловероятно | Низкая |
| **156** | Угроза установки уязвимых версий обновления  программного  обеспечения BIOS | Маловероятно | Низкая |
| **177** | Угроза «фишинга» | Маловероятно | Низкая |
| **161** | Угроза  «форсированного веб- браузинга» | Маловероятно | Низкая |

# Оценка опасности и актуальности угроз предложенной информационной системы

|  |  |  |  |
| --- | --- | --- | --- |
| **№ УБИ** | **Угрозы**  **безопасности ПДн** | **Показатель опасности угрозы** | **Актуальность угрозы** |
|  | | | |
| **170** | Угроза «кражи»  учётной записи | Средний | Неактуальна |

|  |  |  |  |
| --- | --- | --- | --- |
|  | доступа к сетевым сервисам |  |  |
| **158** | Угроза утраты носителей  информации | Средняя | Актуальна |
| **141** | Угроза преодоления физической защиты | Высокий | Актуальна |
| **20** | Угроза загрузки нештатной операционной  системы | Средний | Актуальна |
| **88** | Угроза  несанкционированно го изменения аутентификационной информации | Высокий | Актуальна |
| **93** | Угроза  несанкционированно го редактирования реестра | Низкий | Неактуальна |
| **212** | Угроза нарушения работы  информационной  системы, вызванного обновлением  используемого в ней программного  обеспечения | Средний | Неактуальна |
| **156** | Угроза установки уязвимых версий обновления  программного  обеспечения BIOS | Средний | Неактуальна |
| **177** | Угроза «фишинга» | Средний | Неактуальна |

|  |  |  |  |
| --- | --- | --- | --- |
| **161** | Угроза  «форсированного веб-браузинга» | Средний | Неактуальна |

**Классификация системы**

Компания «DNS» занимается продажей техники. У компании есть свой специально разработанное приложение «DNS». Все остальные программы и приложения декларированы. «DNS» обрабатывает небольшое количество заказов ежемесячно, <<100000. Для оформления заказа «DNS» хранит фамилию имя отчество; паспортные данные; адрес проживания/адрес доставки; номер телефона; список заказов каждого клиента.

Исходя из данных, описанных выше, возможно классифицировать ИСПДн в соответствии с постановлением правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

ИСПДн является информационной системой, обрабатывающей общедоступные данные. Количество обрабатываемых субъектов менее 100000. Руководителем организации был определен 3 тип актуальных угроз. Следовательно, можно сделать вывод, что данная ИСПДн имеет 4 уровень защищенности и 3 тип актуальных угроз. Относительно уровня защищенности объекта возможно определить необходимые организационные и технические меры по обеспечению безопасности, регламентированные приказом ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

# СОСТАВ И СОДЕРЖАНИЕ

**МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

|  |  |  |
| --- | --- | --- |
| Условное обозначен ие и номер меры | Содержание мер по обеспечению безопасности персональных данных | УЗ пд |
| 4 |
| I. Идентификация и аутентификация субъектов доступа и объектов | | |

|  |  |  |
| --- | --- | --- |
| доступа (ИАФ) | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | + |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | + |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и | + |

|  |  |  |
| --- | --- | --- |
|  | лицам, обеспечивающим функционирование информационной системы |  |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | + |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | + |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | + |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | + |
| V. Регистрация событий безопасности (РСБ) | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения | + |
| РСБ.7 | Защита информации о событиях безопасности | + |
| VI. Антивирусная защита (АВЗ) | | |
| АВЗ.1 | Реализация антивирусной защиты | + |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + |
| VIII. Контроль (анализ) защищенности персональных данных (АНЗ) | | |

|  |  |  |
| --- | --- | --- |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + |
| XI. Защита среды виртуализации (ЗСВ) | | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | + |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин | + |
| XII. Защита технических средств (ЗТС) | | |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены | + |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (3ИС) | | |
| ЗИС.3 | Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + |