*Выполнила: Табольская Е. А. БИСО-03-19*

ПОЛИТИКА ИБ Гипермаркета Заря

Компания ООО «Гипермаркет Заря». Штат — 100 сотрудников: 15 - руководство, 20 - бухгалтерия, 10 — IT-отдел, 15 — мерчендайзер, 22 – кассир, 10 – охрана, 8 - менеджер. Управление компании использует телефонную связь, MS Office, Microsoft Money, Антивирус Касперского, 1С: Предприятие, 1С: Бухгалтерия, т. д.

Руководство использует телефонную связь, MS Office, Антивирус Касперского, 1С: Предприятие.

IT-отдел обеспечивает функционирование внутренней сети организации, а также сайта компании и личных кабинетов клиентов. Менеджеры по работе с клиентами осуществляют работу с ними посредством интернета или телефонной связи. Бухгалтерия занимается ведением финансового учета, документооборотом, подготовкой и отправкой отчетности в контролирующие органы. Мерчендайзеры контролируют количественный состав товара на полке, выкладку товара согласно корпоративной планограмме, поддерживают торговый запас, корректируют розничные цены на товар, решают локальные проблемы в точке продажи и др.

Содержание

[1. Общие положения 3](#_Toc53423483)

[2. Принципы и условия обработки персональных данных 3](#_Toc53423484)

[3. Цели обеспечения и управления информационной безопасностью 4](#_Toc53423485)

[4. Обеспечение информационной безопасности 4](#_Toc53423486)

# 1. Общие положения

* 1. Настоящая Политика определяет порядок, условия обработки и меры по обеспечению безопасности персональных данных в ООО «Гипермаркет Заря» (далее - Компания) с целью защиты прав и свобод человека и гражданина при обработке его персональных данных (далее - ПДн), в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
  2. Действие Политики распространяется на все обрабатываемые в Компании с применением средств автоматизации и без применения таких средств ПДн.
  3. Целью создания Политики является ознакомление граждан с принципами, на которых строится обработка ПДн в Компании.
  4. Должностные лица Компании, виновные в нарушении норм, регулирующих обработку и защиту ПДн, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность.
  5. К настоящей Политике должен иметь доступ любой субъект ПДн.

# 2. Принципы и условия обработки персональных данных

Безопасность ПДн, обрабатываемых Компанией, обеспечивается реализацией правовых, организационных, технических и программных мер.

В Компании обрабатываются ПДн следующих субъектов ПДн:

1. Работников, состоящих с Компанией в трудовых отношениях;
2. близких родственников Работников Компании;
3. стажеров и субъектов, проходящих производственную практику в Компании.

Обработка ПДн в Компании осуществляется на законной и справедливой основе согласно следующим принципам:

1. обработке подлежат данные, содержание и объем которых отвечают целям их обработки;
2. должна быть обеспечена точность данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки;
3. данные должны быть уничтожены либо обезличены по достижении целей их обработки или при утрате необходимости в достижении этих целей.

Компания обязана обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ.

# 3. Цели обеспечения и управления информационной безопасностью

Под обеспечением информационной безопасности понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

Основными целями в области обеспечения и управления информационной безопасностью Компании являются:

1. Обеспечение целостности, доступности и конфиденциальности критичной информации, а также обеспечение доступности критичных ИТ-сервисов Компании.
2. Применение обоснованных, экономически эффективных организационных и технических мер по обеспечению информационной безопасности.
3. Соответствие процессов обеспечения информационной безопасности бизнес-требованиям Компании.
4. Обеспечение доверия клиентов и партнеров Компании

# 4. Обеспечение информационной безопасности

Информация является важным активом Компании и ее защита является обязанностью каждого сотрудника.

Доступ к информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.

Для каждого информационного ресурса определяется владелец, отвечающий за предоставление к нему доступа и эффективное функционирование мер защиты информации.

Сотрудники Компании проходят регулярное обучение в области информационной безопасности.

Специалисты информационной безопасности отвечают за определение детальных требований информационной безопасности и контролируют их исполнение в Компании.

Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.