Heineken
Russia

ООО «Объединенные Пивоварни Хейнекен»

Разработал:
Менеджер по аудиту и
информационной безопасности
ООО «Объединенные пивоварни
Хейнекен»

Поточкин С.В.

Утверждаю:
Менеджер службы информационных
технологий
ООО «Объединенные пивоварни Хейнекен»

Левчук А.Ю..

«_12_» января 2011

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ООО «ОБЪЕДИНЕННЫЕ ПИВОВАРНИ ХЕЙНЕКЕН»

Санкт – Петербург

2011

Содержание

Общие положения ... 5
Назначение документа ... 5
Область действия документа ... 6
Порядок ввода в действие и изменение Положения ... 6
Цели и правовое основание обработки персональных данных ... 7
Информационные системы персональных данных ... 8
Состав, категории и местонахождение ПДн ... 8
Организация защиты персональных данных ... 9
Общие положения ... 9
Оценка обстановки ... 10
Обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн ... 11
Обоснование требований по обеспечению безопасности ПДн ... 11
Задачи защиты ПДн ... 12
Замысел обеспечения безопасности ... 12
Основные направления по защите ПДн ... 12
Способы защиты ПДн ... 13
Основные вопросы управления защитой ПДн ... 15
Вопросы обеспечения защиты ПДн ... 16
Организация и проведение работ по созданию и поддержке СЗПДн ... 17
Защита ПДн, находящихся на твердых копиях ... 18
Ответственность и обязанности по обеспечению безопасности ПДн ... 20
Права и обязанности субъектов ПДн ... 20
Субъекты ПДн - работники Общества ... 20
Иные субъекты ПДн (клиенты/контрагенты, аффилированные лица Общество) ... 22
Ответственность ... 22
Контроль соблюдения условий и правил обработки ПДн и их защиты. Порядок расследований нарушений режимов обработки и защиты ПДн ... 24
Общие положения ... 24
Профилактика нарушений ... 24
Порядок расследования нарушений ... 24
Контроль ... 25

Приостановка (отказ) предоставления ПДн 27

Допуск к ПДн. Порядок актуализации знаний, умений, навыков работников при обращении с ПДн 28

Организация допуска к ПДн 28

Порядок актуализации знаний по работе с ПДн 29

Определения и сокращения

ПДн	Персональные данные
ИСПДн	Информационная система персональных данных
СЗПДн	Система защиты персональных данных
Блокирование персональных данных	Временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи
Информационная система персональных данных	Информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств
Использование персональных данных	Действия (операции) с персональными данными, совершаемые Общество в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц
Конфиденциальность персональных данных	Обязательное для соблюдения Общество или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания
Обезличивание персональных данных	Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных
Обработка персональных данных	Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных
Общедоступные персональные данные	Персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности
Персональные данные	Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация
Распространение персональных данных	Действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом
Уничтожение персональных данных	Действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных

Общие положения

Назначение документа

Настоящее Положение определяет порядок организации работ по обработке и защите персональных данных, обрабатываемых в ООО «Объединенные пивоварни Хейнекен» (далее по тексту Общество).

Правовые и нормативно-методические источники документа

1.2.1. Настоящее Положение разработано в соответствии со следующими нормативно-правовыми документами:

- Статья 24 Конституции Российской Федерации;
- Глава 14 Трудового Кодекса Российской Федерации;
- Федеральный закон Российской Федерации №152-ФЗ «О персональных данных» от 27.07.2006 г.;
- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г.;
- Постановление Правительства Российской Федерации «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» № 781 от 17 ноября 2007 г.;
- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Совместный приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;
- Методические рекомендации ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных

системах персональных данных» (Утверждены Заместителем директора ФСТЭК России 15 февраля 2008 г.);

- Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Методические рекомендации ФСТЭК России «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Утверждены Заместителем директора ФСТЭК России 15 февраля 2008 г.);
- Методические рекомендации ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» (Утверждены Заместителем директора ФСТЭК России 15 февраля 2008 г.).

Область действия документа

1.3.1. Положения настоящего документа обязательны для исполнения всеми сотрудниками Общества, филиалов и обособленных структурных подразделений, контрагентами и третьими сторонами, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования по защите персональных данных.

1.3.2. Действие настоящего документа распространяется на все информационные системы персональных данных Общества.

Порядок ввода в действие и изменение Положения

1.5.1. Настоящее Положение вступает в силу с момента его утверждения Обществе в установленном порядке.

1.5.2. Все изменения в Положение вносятся приказом.

Цели и правовое основание обработки персональных данных

2.1. Обработка персональных данных работников Общество может осуществляться в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, в т.ч. Трудового Кодекса Российской Федерации, Федерального Закона №152-ФЗ «О персональных данных», содействия работникам в выполнении ими своих функциональных обязанностей, обучении, продвижении по работе, обеспечения личной безопасности работника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Общества, очередности предоставления отпусков, установления и расчета размера заработной платы, страхования работников, оформления страховых свидетельств государственного пенсионного страхования, а также в иных целях, необходимых Обществу в связи с трудовыми отношениями с работниками Общества.

2.2. Обработка персональных данных субъектов персональных данных, не являющихся работниками Общества, осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, выполнения работ и предоставления услуг, определенных Уставом и лицензиями Общества, выполнения договорных обязательств Общества перед клиентами, предоставления возможности работникам контрагентов Общества выполнения обязанностей, предусмотренных договорами между Обществом и его контрагентами.

Информационные системы персональных данных

Состав, категории и местонахождение ПДн определяют замысел защиты при обработке ПДн в ИСПДн Общества.

Состав, категории и местонахождение ПДн

3.1.1. В Обществе обрабатываются персональные данные следующих субъектов ПДн:

- работники Общества;
- иные субъекты ПДн – клиенты (контрагенты) Общества, аффилированные лица Общества.

3.1.2. Персональные данные работников Общества содержатся в документах персонального учета работников – личном деле, трудовой книжке, выдаваемых доверенностях (при наличии), а также в иных документах, формируемых в процессе осуществления профессиональной деятельности отделов персонала Общества, филиалов и обособленных подразделений. Персональные данные работников содержатся также в информационных системах Общества, доступ к которым предоставлен ограниченному кругу работников Общества.

3.1.3. ПДн клиентов (контрагентов) Общества содержатся в заключаемых с ними договорах, документах, относящихся к исполнению данных договоров, и ИСПДн.

3.1.4. Местонахождение ПДн определяется, исходя из требований, предъявляемых к форме представления ПДн. Им является:

- В случае автоматизированной обработки:
  - сервера приложений ИСПДн;
  - АРМ пользователей ИСПДн;
  - съемные носители, содержащие ПДн.
- В случае неавтоматизированной обработки:
  - твердые копии, содержащие ПДн.

Организация защиты персональных данных

Общие положения

4.1.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

4.1.2. Обеспечение безопасности ПДн при их обработке в автоматизированных ИСПДн проводится путем выполнения комплекса организационных и технических мероприятий (применения технических средств) в рамках системы (подсистемы) защиты персональных данных, развертываемой в ИСПДн в процессе ее создания или модернизации

4.1.3. Организация защиты ПДн подразумевает проведение мероприятий, направленных на недопущение несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

4.1.4. Порядок организации обеспечения безопасности ПДн в ИСПДн предусматривает:

- оценку обстановки;
- обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;
- разработку замысла обеспечения безопасности ПДн;
- выбор целесообразных способов (мер и средств) защиты ПДн;

- решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;
- обеспечение реализации принятого замысла защиты;
- планирование мероприятий по защите ПДн;
- организацию и проведение работ по созданию системы защиты персональных данных (СЗПДн) в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в ИСПДн, решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;
- разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн;
- развертывание и ввод в опытную эксплуатацию СЗПДн в ИСПДн;
- доработку СЗПДн по результатам опытной эксплуатации.

Оценка обстановки

4.2.1. Оценка обстановки основывается на результатах комплексного обследования ИСПДн, в ходе которого, в т.ч., проводится определение защищаемой информации и ее категорирование.

4.2.2. При оценке обстановки определяется необходимость обеспечения безопасности ПДн от угроз:

- уничтожения, хищения аппаратных средств ИСПДн, носителей информации путем физического доступа к элементам ИСПДн;
- утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН);
- перехвата при передаче по проводным (кабельным) линиям связи;
- хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-

аппаратных и программных средств (в том числе программно-математических воздействий);

- воспрепятствования функционированию ИСПДн путем преднамеренного электромагнитного воздействия на ее элементы;
- непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

4.2.3. При оценке обстановки учитывается степень ущерба, который может быть причинен в случае неправомерного использования соответствующих ПДн, а также проводится анализ имеющихся в распоряжении мер и средств защиты ПДн.

Обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн

Обоснование требований по обеспечению безопасности ПДн

4.3.1.1. Обоснование требований по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, проводится в соответствии с нормативными и методическими документами уполномоченных федеральных органов исполнительной власти, обязательными к применению стандартами и на основании методического документа «Положение о методах и способах защиты информации в информационных системах персональных данных», утвержденное Приказом ФСТЭК России от 5 февраля 2010 г. № 58. При этом выявление и оценка актуальности угроз безопасности персональных данных при их обработке в ИСПДн осуществляется в соответствии с методическими документами ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14.02.2008 года и «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008 года.

Задачи защиты ПДн

4.3.2.1. СЗПДн ИСПДн Общества предназначена для решения следующих задач по защите от НСД:

- идентификация пользователя в системе;
- проверка прав доступа к защищаемым данным в рамках общезначимого (системного) контекста безопасности;
- обеспечение целостности данных;
- предотвращение попыток получения НСД к ПДн, обрабатываемых в ИСПДн Общества;
- предотвращение утечки информации, содержащей ПДн, а именно:
  - утечка информации, содержащей ПДн, за счет подключения внешних устройств;
- предотвращение несанкционированного, в том числе случайного, уничтожения, изменения, блокирования, копирования, распространения персональных данных.

Замысел обеспечения безопасности

Замысел обеспечения безопасности ПДн определяет:

- основные направления по защите ПДн;
- выбор способов защиты ПДн;
- вопросы управления защитой ПДн;
- вопросы обеспечения защиты ПДн.

Основные направления по защите ПДн

4.4.1.1. Основным направлением по защите ПДн является обеспечение конфиденциальности при обработке информации, содержащей ПДн, и обеспечивается:

- проведением мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

- своевременным обнаружением фактов несанкционированного доступа к ПДн;
- недопущением воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянным контролем обеспечения уровня защищенности персональных данных.

4.4.1.2. Обеспечение деятельности по основным направлениям по защите ПДн осуществляется должностными лицами ответственными за информационную безопасность в Общество.

4.4.1.3. Дополнительным направлением по защите ПДн является обеспечение целостности обрабатываемой информации, содержащей ПДн, и обеспечивается:

- проведением мероприятий, направленных на предотвращение несанкционированного изменения или удаления информации, содержащей ПДн;
- возможностью незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.4.1.4. Обеспечение деятельности по дополнительным направлениям по защите ПДн осуществляют подразделения Общество, обеспечивающие функционирование ИС.

Способы защиты ПДн

4.4.2.1. По способам осуществления все меры обеспечения безопасности ПДн при их обработке в ИСПДн подразделяются на правовые, организационные и технические.

4.4.2.2. К правовым мерам относится регламентация законом и нормативными актами действий с информацией и оборудованием, и наступление ответственности за нарушение требований указанных законов и актов.

4.4.2.3. К организационным относятся меры, регламентирующие процессы функционирования ИСПДн, порядок использования ее ресурсов, деятельность персонала,

а также порядок взаимодействия пользователей с системой таким образом, чтобы максимально снизить возможность угроз безопасности ПДн. Организационные меры включают:

- мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);
- мероприятия, осуществляемые при подборе и подготовке персонала, обслуживающего ИСПДн;
- организацию охраны и режима допуска к элементам ИСПДн;
- организацию учета, хранения, использования и уничтожения документов и носителей информации, содержащей ПДн.

4.4.2.4. К техническим мерам относятся аппаратные, программные и программно-аппаратные средства защиты, выполняющие (самостоятельно или в комплексе с другими средствами) функции СЗПДн:

- идентификацию и аутентификацию пользователей;
- разграничение доступа к ресурсам;
- обеспечение безопасного межсетевого взаимодействия элементов ИСПДн;
- регистрацию событий;
- обеспечение целостности системы;
- контроль отсутствия вредоносного программного обеспечения;
- криптографическую защиту[1] передаваемой информации и каналов связи;
- анализ защищенности;
- обнаружение вторжений[2];
- создание резервных копий информации, содержащей ПДн.

[1] Мероприятия по криптографической защите ПДн проводятся в соответствии с требованиями нормативных документов по защите ПДн Федеральной службы безопасности Российской Федерации.
[2] Мероприятия по обнаружению вторжений в ИСПДн проводятся в соответствии с требованиями нормативных документов Федеральной службы безопасности Российской Федерации.

Основные вопросы управления защитой ПДн

4.4.3.1. Под основными вопросами управления защитой ПДн понимается перечень вопросов, связанных с:

- распределением функций управления доступом к данным и их обработкой между должностными лицами;
- определением порядка изменения правил доступа к защищаемой информации;
- определением порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;
- определением порядка действий должностных лиц в случае возникновения нештатных ситуаций;
- определением порядка проведения контрольных мероприятий и действий по его результатам.

4.4.3.2. Распределение обязанностей по основным вопросам управления защитой ПДн при их обработке в ИСПДн, осуществляется следующим образом:

- распределение функций управления доступом к ПДн и их обработкой осуществляется владельцами активов Общества;
- контроль корректности и достаточности осуществляют должностные лица ответственные за информационную безопасность в Обществе.

4.4.3.3. Должностные лица ответственные за информационную безопасность в Обществе также осуществляют следующие действия:

- определяют порядок изменения правил доступа к защищаемой информации;
- определяют порядок изменения правил доступа к резервируемым информационным и аппаратным ресурсам;
- определяют порядок действий должностных лиц в случае возникновения нештатных ситуаций;

Вопросы обеспечения защиты ПДн

Вопросы, связанные с обеспечением замысла защиты ПДн в части финансирования, технической, программной и информационной поддержки распределяются следующим образом:

4.4.4.1. Руководство Общества:

- утверждает финансирование программ в области защиты конфиденциальной информации;
- определяет полномочия подразделений Общества в части защиты ПДн.

4.4.4.2. Должностные лица ответственные за безопасность в Обществе:

- осуществляют методическое обеспечение и информационную поддержку в области защиты ПДн;
- организуют исполнение пунктов данного Положения;
- организуют разработку и выполнение программ в области защиты ПДн;
- осуществляют в пределах своей компетенции проведение проверочных мероприятий в отношении персонала Общества, допущенного к обработке ПДн;
- устанавливают порядок определения размеров ущерба, наступившего из-за несанкционированного, в том числе случайного, доступа к ПДн, результатом которого стало уничтожение, изменение, блокирование, копирование, распространение персональных данных;
- принимают меры по выполнению договоров о совместном использовании и защите ПДн, принимает решения о возможности передачи носителей информации, содержащей ПДн, другим лицам (контрагентам и третьим сторонам) или государственным организациям;
- в пределах своих полномочий решают иные вопросы, возникающие при защите ПДн при их обработке в ИСПДн Общества.

4.4.4.3. Функциональные структурные подразделения Общества:

- обеспечивают защиту ПДн субъектов, переданных им другими подразделениями (работниками), контрагентами, третьими лицами, учреждениями и организациями;
- обеспечивают защиту ПДн в подчиненных им подразделениях (на личном участке работ) Общества, в соответствии с требованиями нормативно-правовой документации.

4.4.4.4. Юридическая служба Общества:

- при необходимости инициируют уголовные и гражданские дела о нарушениях при обработке ПДн;
- обеспечивает юридическую защиту подразделений и должностных лиц Общества в связи с их деятельностью по защите ПДн при их обработке в ИСПДн.

4.4.4.5. Руководители структурных подразделений, работники которых имеют доступ к персональным данным, осуществляют контроль защиты персональных данных субъектов ПДн в рамках своих подразделений.

4.4.5. Работники Общества обеспечивают конфиденциальность персональных данных субъектов ПДн, ставших им известными в связи с выполнением своих функциональных обязанностей (за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных).

Организация и проведение работ по созданию и поддержке СЗПДн

4.5.1. Под организацией и проведением работ по созданию и поддержке СЗПДн подразумевается комплекс административных и технических мер, направленных на проектирование, внедрение, эксплуатацию и поддержку СЗПДн.

4.5.2. Организацию и проведение работ по созданию и поддержке СЗПДн осуществляют должностные лица ответственные за информационную безопасность в Обществе в рамках своей компетенции.

4.5.3. Перечень мероприятий, необходимых для организации и проведения работ по созданию и поддержке СЗПДн, перечислен в документе «Требования по защите персональных данных при их обработке в информационных систем персональных данных ООО «Объединенные пивоварни Хейнекен».

4.5.4. Испытания СЗПДН проводятся в процессе развертывания и ввода в опытную эксплуатацию ИСПДн в соответствии с частным техническим заданием. Заключение по результатам испытаний должно содержать вывод о степени соответствия СЗПДн заданным требованиям по обеспечению безопасности ПДн.

4.5.5. По результатам проведения опытной эксплуатации СЗПДн при необходимости проводится доработка системы.

4.5.6. При подготовке документации по вопросам обеспечения безопасности ПДн при их обработке в ИСПДн и эксплуатации СЗПДн в обязательном порядке также разрабатываются:

- требования по обеспечению безопасности ПДн при обработке в ИСПДн;
- должностные инструкции персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн;
- рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

Защита ПДн, находящихся на твердых копиях

4.6.1. При создании твердой копии ПДн не допускается фиксация в копии ПДн, цели обработки которых заведомо не совместимы.

4.6.2. В отношении информации, содержащей ПДн, и находящейся на твердых копиях, выполняются следующие мероприятия:

- хранение твердых копий ПДн, обрабатываемых в ПДн, осуществляется в специальных местах, определенных должностными лицами ответственными за информационную безопасность в Общество и утвержденных руководством Общества;

- доступ к месту хранения твердых копий должен быть ограничен использованием средств физического доступа (кодовые замки, система видеонаблюдения);
- допуск к местам хранения твердых копий ПДн осуществляется на основании утвержденного списка;
- уничтожение твердых копий ПДн должно осуществляться таким образом, чтобы исключить дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на твердой копии (удаление, вымарывание).

Ответственность и обязанности по обеспечению безопасности ПДн

Права и обязанности субъектов ПДн

Субъекты ПДн - работники Общества

5.1.1.1. Работники имеют право:

- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением. Работник при отказе кадрового органа исключить или исправить его персональные данные имеет право заявить в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требовать от Общества уведомления всех лиц, которым ранее были сообщены неверные или неполные их персональные данные, обо всех произведенных в них изменениях или исключениях из них;
- обжаловать действия или бездействие работников Общества в установленном законом порядке, если работник, являющийся субъектом персональных данных, считает, что обработка его персональных данных осуществляется с нарушением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы.

5.1.1.2. Работник обязуется:

- предоставлять в Общество достоверные, документированные персональные данные, соответствующие действительности;
- своевременно сообщать Общество в документарном виде об изменении своих персональных данных;
- соблюдать правила обращения с документами, содержащими персональные данные, порядок их получения, обработки и хранения;
- строго соблюдать установленные в Обществе правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- во время работы с документами, содержащими ПД, исключать возможность ознакомления с ними иных лиц, не имеющих доступа к данным документам;
- при увольнении сдать руководителю структурного подразделения (заместителю руководителя, специально назначенному лицу) все имеющиеся в его распоряжении материальные носители информации, содержащей персональные данные;
- обеспечивать конфиденциальность персональных данных субъектов ПДн, ставших им известными в связи с выполнением своих функциональных обязанностей (за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных).

5.1.1.3. Работникам запрещается:

- выносить документы и другие носители, содержащие персональные данные, за пределы территории Общества без разрешения руководителя структурного подразделения;
- знакомить работников других структурных подразделений, не имеющих доступа к персональным данным субъектов ПДн по своим функциональным обязанностям, с документами, содержащими персональные данные, без письменного разрешения (резолюции) руководителя структурного подразделения Общество, а представителей клиентов и иных организаций – без наличия письменного согласия субъекта ПД (за исключением случаев,

когда передача персональных данных субъекта без его согласия допускается действующим законодательством РФ);

- передавать информацию, содержащую персональные данные, по каналам телефонной и факсимильной связи, с использованием сетей Интернет, Интранет, если меры по защите информации не приняты;
- сообщать кому-либо свой пароль или передавать пароль для доступа к ресурсам ИСПДн;
- использовать чужое имя пользователя и пароль для доступа к ресурсам ИСПДн.

Иные субъекты ПДн (клиенты/контрагенты, аффилированные лица Общество)

5.1.2.1. Субъект, персональные данные которого обрабатываются в Обществе, имеет право:

- Получать доступ к своим персональным данным и ознакомляться с ними.
- Получать от Общества:
  - сведения о лицах (только должности), которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
  - перечень обрабатываемых персональных данных и источник их получения;
  - сроки обработки персональных данных, в том числе сроки их хранения;
  - сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.
- Обжаловать в установленном законом порядке неправомерные действия или бездействие Общество при обработке и защите его персональных данных.

Ответственность

5.2.1. Работник, которому в силу трудовых отношений с Обществом стала известна информация, составляющая персональные данные, в случае нарушения режима

защиты этих персональных данных несет материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами Российской Федерации.

5.2.2. Разглашение персональных данных субъектов ПДн (передача их посторонним лицам, в том числе работникам Общества, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативными актами (приказами, распоряжениями) Общества, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарного взыскания, если иное не предусмотрено законодательством РФ.

5.2.3. Работник Общества, имеющий доступ к персональным данным субъектов и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Общество(п.7 ст.243 Трудового кодекса РФ).

5.2.4. Работники Общество, имеющие доступ к персональным данным субъектов, виновные в незаконном разглашении или использовании персональных данных лиц без согласия субъектов из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса РФ.

5.2.5. Ответственность за организацию защиты ПДн возлагается на руководителя Общества.

Контроль соблюдения условий и правил обработки ПДн и их защиты. Порядок расследований нарушений режимов обработки и защиты ПДн

Общие положения

6.1.1. Контроль за обеспечением защиты персональных данных осуществляют руководство Общества, подразделение (должностное лицо), ответственное за обеспечение безопасности ПДн в Обществе в рамках компетенции в соответствии с действующим законодательством РФ, а также действующими внутренними нормативными документами Общества.

6.1.2. Контроль за соблюдением законодательства РФ при обеспечении защиты ПДн и законностью принимаемых при этом решений осуществляет Юридическая служба Общества.

Профилактика нарушений

6.2.1. В программу профилактики нарушений входят мероприятия, направленные на:

- доведения до персонала Общества, допущенного до обработки ПДн, всей важности и необходимости выполнения задач по защите ПДн в рамках компетенции персонала Общества;
- проведением плановых и внеплановых проверок с целью выявления нарушений или предпосылок к нарушениям при обработке ПДн;
- доведением до всего персонала Общества результатов проведения проверок (в определенных случаях).

Порядок расследования нарушений

6.3.1. При обнаружении инцидентов, связанных с нарушением требований по защите ПДн, в обязательном порядке оповещается подразделений (должностное лицо), ответственное за обеспечение безопасности ПДн в Обществе.

6.3.2. После получения сообщения о произошедшем инциденте (либо подозрении на него), указанный работник фиксирует сообщение и организует расследование инцидента.

6.3.3. Расследование нарушений осуществляется комиссией, в состав которой входят представители подразделения (должностное лицо), ответственного за обеспечение безопасности ПДн в Обществе, подразделения в котором произошло нарушения и Дирекции по информационным технологиям. При необходимости в качестве экспертов могут привлекаться работники других подразделения Общества.

6.3.4. Результаты работы комиссии оформляются в виде заключения с рекомендациями, которое утверждается руководителем Общества, после чего принимаются меры по недопущению повторения подобных нарушений.

Контроль

6.4.1. Внутренние проверки проводятся в подразделениях Общество, участвующих в обработке ПДн, не реже 2-х раз в год в соответствии с Планом проверки.

6.4.2. Внутренние проверки проводятся для:

- обеспечения соответствия требованиям настоящего Положения, а также других нормативных документов по защите ПДн (внутрикорпоративным, законодательным);
- подтверждения эффективного внедрения и поддержания системы защиты ПДн;
- обеспечения функционирования системы защиты ПДн в соответствии с ожиданиями.

6.4.3. Организацию и проведение внутренних проверок осуществляют должностные лица ответственные за информационную безопасность (обеспечение безопасности персональных данных) в Обществе.

6.4.4. Указанным подразделением разрабатывается годовой План (в т.ч. состав проверок, очередность и даты проведения) проведения проверок, который

согласовывается и утверждается руководством Общества. После чего утвержденный План проверок рассылается руководителям проверяемых структурных подразделений.

6.4.5. При проведении проверки должен присутствовать представитель проверяемого подразделения.

6.4.6. Заключение о состоянии ИБ по результатам проверки и выявленные несоответствия заносятся проверяющим в Отчет по результатам проверки, который согласовывается с руководством Общество.

6.4.7. В случае выявления несоответствий Общество организуется расследование причин нарушения и принимаются меры по недопущению повторения ситуаций.

Приостановка (отказ) предоставления ПДн

7.1. При обнаружении нарушений порядка предоставления ПДн подразделение, ответственное за обеспечение безопасности ПДн Общества незамедлительно приостанавливают предоставление ПДн пользователям информационной системы до выявления причин нарушений и устранения этих причин.

Допуск к ПДн. Порядок актуализации знаний, умений, навыков работников при обращении с ПДн

Организация допуска к ПДн

8.1.1. Доступ к персональным данным субъекта имеют работники Общества, которым персональные данные необходимы в связи с исполнением ими трудовых обязанностей. Перечень работников, имеющих доступ к персональным данным, определяется руководством Общество по представлению заместителей и руководителей структурных подразделений Общество и утверждается приказом по Обществу.

8.1.2. Доступ к персональным данным субъектов работникам Общества, не включенным в указанный выше перечень, может быть предоставлен в целях выполнения порученного задания и на основании служебной записки с положительной резолюцией руководства Общество. Служебная записка должна содержать объем и срок предоставления доступа.

8.1.3. В случае, если Обществу оказывают услуги юридические и физические лица на основании заключенных договоров, в силу которых им может быть предоставлен доступ к конфиденциальной информации (в т.ч. к персональным данным субъектов), то до начала работ должно быть подписано соглашение о неразглашении конфиденциальной информации между Обществом и указанными физическими или юридическими лицами.

8.1.4. Процедура оформления допуска к персональным данным включает в себя:

- принятие на себя обязательств перед Обществом по нераспространению доверенных им сведений, составляющих конфиденциальную информацию (отражаются в трудовом договоре). В случае, если работнику оформляется допуск на основании служебной записки - истребование с работника письменного обязательства о соблюдении конфиденциальности персональных данных субъектов ПДн и соблюдении правил их обработки.
- письменное согласие на проведение в отношении их подразделениями безопасности проверочных мероприятий;

- ознакомление работника под подпись с настоящим Положением

Примечание. При наличии иных нормативных актов (приказы, распоряжения, инструкции и т.п.), регулирующих обработку и защиту персональных данных субъекта, также производится ознакомление с ними работника под подпись;

- принятие решения руководителем Общества о допуске оформляемого лица к ПДн.

8.1.5. Доступ к персональным данным субъектов других работников Общества, не имеющих надлежащим образом оформленного допуска, запрещается.

Порядок актуализации знаний по работе с ПДн

8.2.1. Обучение работникам правилам обращения с ПДн может быть:

- первичным - при принятии на работу;
- периодическим.

8.2.2. Первичное обучение включает инструктаж нового работника по правилам работы с ПДн, принятым в Обществе, во время которого работник под подпись знакомится с нормативными и организационно-распорядительными документами Общества по ИБ в части, его касающейся. Инструктаж проводится должностным лицом ответственным за информационную безопасность в Обществе (либо работником Отдела персонала Общества, филиала, обособленного подразделения).

8.2.3. Периодическое обучение организуется в соответствии с Политикой обучения и повышении осведомленности сотрудников ООО «Объединенные пивоварни Хейнекен» в вопросах информационной безопасности:

8.2.4. Проведение внепланового обучения работников возможно в случаях:

- внесения существенных изменений в организационно-распорядительную документацию по защите ПДн Общества;
- возникновения инцидентов, в том числе нарушений правил по работе с ПДн, принятых в Обществе (по выяснении причин произошедшего);

- запросов руководителей подразделений;
- возникновения инцидентов, критических ситуаций, т.п. (по выяснении причин произошедшего).