DIR-17285-540775

УТВЕРЖДЕН
Приказом от 27.06.2014 №14.06/27.3-ОД
Вступает в силу с 01 июля 2014 года

ПОЛИТИКА

обработки и обеспечения безопасности персональных данных в ОАО «Брокерский дом «ОТКРЫТИЕ»

Москва 2014

СОДЕРЖАНИЕ:

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 3
1. ОБЩИЕ ПОЛОЖЕНИЯ 3
2. ЦЕЛИ ОБРАБОТКИ ПДН 3
3. ПОРЯДОК СБОРА И ОБРАБОТКИ ПДН 4
4. ОСНОВНЫЕ НАПРАВЛЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН 7
5. ОСНОВНЫЕ СПОСОБЫ И МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН 7
6. ДОЛЖНОСТНЫЕ ЛИЦА, ОТВЕТСТВЕННЫЕ ЗА ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕЙ ПОЛИТИКИ 8
7. ПОРЯДОК ПРИВЛЕЧЕНИЯ И ВЗАИМОДЕЙСТВИЯ ПОДРАЗДЕЛЕНИЙ КОМПАНИИ, СПЕЦИАЛИЗИРОВАННЫХ СТОРОННИХ ОРГАНИЗАЦИЙ ПРИ РАЗРАБОТКЕ, ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И СРЕДСТВ ЗАЩИТЫ 8
8. ПОРЯДОК РАЗРАБОТКИ, ВВОДА В ДЕЙСТВИЕ И ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ 8
9. ПРАВА И ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ КОМПАНИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН 10
10. ВНУТРЕННИЙ КОНТРОЛЬ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ПДН 12
11. ПОРЯДОК ПУБЛИКАЦИИ И ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ДОКУМЕНТУ 12
12. СООТНОШЕНИЕ ВРЕДА И ПРИНИМАЕМЫХ КОМПАНИИ МЕР 12
13. НОРМАТИВНО-ПРАВОВЫЕ АКТЫ И МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ ПО ЗАЩИТЕ ПДН ПРИ ИХ ОБРАБОТКЕ В ИСПДН 13

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИСПДн – Информационная система персональных данных

НСД – Несанкционированный доступ

ПДн– Персональные данные

СЗПДн – Система защиты персональных данных

СрЗИ – Средство защиты информации

ФСБ России – Федеральная служба безопасности России

ФСТЭК России – Федеральная служба по техническому и экспортному контролю России

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение документа

Настоящая Политика обработки и обеспечения безопасности персональных данных открытого акционерного общества «Брокерский дом «ОТКРЫТИЕ» (далее – Политика) является основным документом по защите персональных данных (ПДн) в Открытом акционерном обществе «Брокерский дом «ОТКРЫТИЕ» (далее – Компании) и определяет цели, порядок организации, планирования и выполнения мероприятий по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных Компании (далее – ИСПДн).

Политика разработана на основании нормативно-правовых актов и методических документов по защите ПДн, перечисленных в разделе 13 настоящей Политики.

Настоящая Политика не отменяет положений и требований иных документов Компании, регламентирующих порядок обращения с информацией ограниченного доступа, не содержащей сведений, составляющих государственную тайну (конфиденциальной информацией).

Политика допускает внесение изменений, вызванных дополнениями (изменениями) нормативно-правовой основы, развитием ИСПДн или изменением условий обработки ПДн. Политика и изменения к ней вводятся в действие приказом генерального директора Компании и вступают в силу с момента подписания приказа.

1.2. Целевая аудитория

Настоящая Политика предназначена для сотрудников подразделений Компании, непосредственно связанных с эксплуатацией ИСПДн и обеспечением безопасности ПДн, руководителей данных подразделений, а также для сотрудников сторонних организаций, допускаемых в установленном порядке к выполнению работ на оборудовании ИСПДн, в т.ч. по модернизации оборудования и программного обеспечения данных систем.

2. ЦЕЛИ ОБРАБОТКИ ПДН

Цели обработки ПДн в Компании являются:

- исполнение трудовых договоров с сотрудниками и выполнение требований трудового законодательства;
- исполнении гражданско-правовых договоров с клиентами.

3. ПОРЯДОК СБОРА И ОБРАБОТКИ ПДН

3.1. Источники получения ПДн

Источниками получения ПДн являются:

- документы, предоставляемые субъектами ПДн при приеме на работу;
- документы, предоставляемые клиентами для заключения договора.
- анкеты, заполняемые клиентами при заключении договора.

3.2. Порядок получения ПДн

Сбор, систематизация и накопление ПДн осуществляется путем занесения ПДн сотрудниками Компании в ИСПДн при оформлении трудовых и гражданско-правовых договоров.

Дальнейшее изменение ПДн клиентов и работников производится по их заявлению в установленном порядке.

3.3. Условия предоставления доступа к ПДн

Лица, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании списка, утвержденного генеральным директором Компании. Доступ к ПДн предоставляется только на период действия указанной необходимости.

Руководители структурных подразделений Компании, в которых сотрудникам нужен доступ к ПДн для выполнения служебных (трудовых) обязанностей, предоставляют списки соответствующих сотрудников своих подразделений лицу осуществляющему функции по организации обработки персональных данных и по обеспечению безопасности персональных данных ПДн при их обработке в ИСПДн (далее – ответственный за обеспечение безопасности ПДн).

Сводный список сотрудников Компании ответственный за обеспечение безопасности ПДн предоставляет генеральному директору Компании на утверждение.

Ответственный за обеспечение безопасности ПДн организовывает мероприятия по периодическому контролю актуальности списков сотрудников Компании, допущенных к работе с ПДн, и контролю соблюдения требований по обеспечению безопасности ПДн этими сотрудниками.

При изменении штатного состава и/или необходимости предоставить или ограничить доступ к ПДн сотрудникам руководитель структурного подразделения уведомляет ответственного за обеспечение безопасности ПДн о необходимости внесения изменений в список лиц, допущенных к обработке ПДн.

Перед предоставлением доступа к ПДн сотрудник Компании обязан:

- под роспись ознакомиться с организационно-распорядительными документами Компании по обработке и обеспечению безопасности ПДн;
- получить всю информацию об ответственности, которую он несет при обработке ПДн;
- ознакомиться с эксплуатационными документами на программные средства информационной системы и средства защиты информации, установленные на его рабочем месте;

- получить основные навыки работы с данными средствами;

- получить контактную информацию о сотрудниках, являющихся ответственными за обеспечение безопасности ПДн, с целью уведомления их в случаях, предусмотренных организационно-распорядительными документами Компании.

Состав лиц, которым разрешен доступ к ПДн, должен быть максимально ограничен. Полномочия по действиям над ПДн должны быть по возможности минимально необходимыми для выполнения служебных обязанностей.

В порядке исключения возможно предоставление доступа к ИСПДн (в рамках выполнения операций по технической поддержке ИСПДн) единичным сотрудникам сторонних организаций с обязательным выполнением всего комплекса организационных и технических мер по обеспечению безопасности ПДн.

3.4. Порядок обработки ПДн

ПДн обрабатываются в Компании:

- с использованием средств автоматизации (в электронном виде);

- без использования средств автоматизации (на бумажных носителях информации).

- в Компании ведутся следующие журналы:

- учета материальных носителей ПДн;

- однократного пропуска посетителей на территорию;

- учета обращений субъектов ПДн.

Заполнение данных журналов возлагается на ответственного за обеспечение безопасности ПДн.

Уничтожение ПДн осуществляется на основании решения, утвержденного генеральным директором Компании с оформлением соответствующего акта об уничтожении ПДн.

3.5. Порядок передачи ПДн третьим лицам

Передача ПДн осуществляется:

- на основании положений действующего законодательства об оперативно-розыскной деятельности – в установленном порядке;

- в органы государственной власти в рамках предоставления государственных услуг в электронном виде. Перечень передаваемых ПДн зависит от конкретной услуги, передача и получение информации регламентируется законодательством, регулирующим предоставление конкретной государственной услуги;

- с юридическими и физическими лицам, в соответствии с договорами и наличием согласия субъектов ПДн.

Факт передачи ПДн третьим лицам зафиксирован в трудовых и гражданско-правовых договорах.

3.6. Порядок обработки ПДн субъектов ПДн после окончания действия договора на оказание услуг

ПДн Клиентов хранятся в ИСПДн в течение 5 лет.

ПДн работников хранятся в Компании 75 лет.

3.7. Порядок обеспечения права субъекта ПДн на доступ к своим ПДн

Поступающие запросы (обращения) субъектов ПДн на получение сведений об обработке своих ПДн, а также об уточнении, блокировании или уничтожении своих ПДн регистрируются в журнале обращений субъектов ПДн и передаются на рассмотрение уполномоченному лицу.

Доступ к своим ПДн предоставляется субъекту ПДн или его законному представителю при обращении либо при получении запроса субъекта ПДн или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПДн или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Ответ на запрос субъекта ПДн на получение своих ПДн должен содержать в доступной форме сведения о наличии ПДн субъекта в Компании, и в нем не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

Субъект ПДн имеет право на получение при обращении или при получении запроса информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Компанией;
- правовые основания и цели обработки ПДн;
- цели и применяемые Компанией способы обработки ПДн;
- наименование и место нахождения Компании, сведения о лицах (за исключением сотрудников Компании), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Компанией или на основании федерального закона);
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- информацию об осуществленной или предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Компании, если обработке поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

- Возможность ознакомления с ПДн предоставляется при обращении субъекта ПДн или его законного представителя в течение тридцати рабочих дней с даты получения запроса субъекта ПДн или его законного представителя.

Субъект ПДн вправе требовать уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. Соответствующие действия выполняются уполномоченным лицом в установленном порядке по предоставлению субъектом ПДн или его законным представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту, и обработка которых осуществляется в Компании, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах уведомляется субъект ПДн или его законный представитель и третьи лица, которым ПДн этого субъекта были переданы.

4. ОСНОВНЫЕ НАПРАВЛЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

Основными направлениями работ по обеспечению безопасности ПДн в Компании являются:

- предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права на доступ к ним;
- разработка и практическая реализация организационных и технических мероприятий по защите:
- ПДн, обрабатываемых средствами вычислительной техники;
- ПДн, выводимых на экраны видеомониторов;
- ПДн, хранящихся на физических носителях, в том числе входящих в состав автоматизированных систем;
- ПДн, передаваемых по каналам связи, выходящим за пределы контролируемой зоны;
- своевременное обнаружение фактов несанкционированного доступа к ПДн;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к ПДн;
- постоянный контроль за обеспечением уровня защищенности ПДн.

5. ОСНОВНЫЕ СПОСОБЫ И МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

Основными способами и мерами по обеспечению безопасности ПДн в Компании являются:

- привлечение лицензиатов ФСТЭК России для выполнения работ по технической защите ПДн, либо лицензирование деятельности в области защиты конфиденциальной информации;
- противодействие утечке по техническим каналам, несанкционированному доступу, программно-техническому воздействию с целью нарушения конфиденциальности, целостности и доступности защищаемой информации в процессе ее обработки, передачи и хранения;
- применение автоматизированных систем в защищенном исполнении для обработки, хранения и передачи ПДн;

- использование сертифицированных средств защиты информации и контроль их эффективности;

- аттестация и/или аудит объектов информатизации по требованиям безопасности информации.

6. ДОЛЖНОСТНЫЕ ЛИЦА, ОТВЕТСТВЕННЫЕ ЗА ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕЙ ПОЛИТИКИ

Всю полноту ответственности за обеспечение безопасности ПДн в Компании несет его генеральный директор. Сотрудники, допущенные к работе с ПДн, несут ответственность за выполнение требований настоящей Политики и других локальных нормативных актов по организации процесса обработки ПДн в части, их касающейся.

Организационно-методическое руководство работами по обеспечению безопасности ПДн, выполнение работ и контролю выполнения требований настоящей Политики возложено на ответственного за обеспечение безопасности ПДн.

7. ПОРЯДОК ПРИВЛЕЧЕНИЯ И ВЗАИМОДЕЙСТВИЯ ПОДРАЗДЕЛЕНИЙ КОМПАНИИ, СПЕЦИАЛИЗИРОВАННЫХ СТОРОННИХ ОРГАНИЗАЦИЙ ПРИ РАЗРАБОТКЕ, ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ И СРЕДСТВ ЗАЩИТЫ

Для выполнения мероприятий по обеспечению безопасности ПДн могут привлекаться специализированные организации, имеющие соответствующие лицензии ФСТЭК и/или ФСБ России.

При выполнении отдельных видов работ обеспечению безопасности ПДн с привлечением специализированных организаций в Компании определяются подразделения (или отдельные сотрудники), ответственные за организацию и проведение этих работ.

Планируемые мероприятия по обеспечению безопасности ПДн разрабатываются ответственными за обеспечение безопасности ПДн (сотрудниками подразделения, осуществляющего функции по организации защиты персональных данных) и включаются отдельным разделом в годовой план мероприятий по обеспечению безопасности ПДн в Компании.

Раздел плана по обеспечению безопасности ПДн должен включать следующие подразделы:

- мероприятия по выполнению решений ФСТЭК России, приказов и распоряжений вышестоящей организации по обеспечению безопасности ПДн;

- мероприятия по обеспечению безопасности ПДн в структурных подразделениях Компании;

- организационно-методическое обеспечение работ по обеспечению безопасности ПДн (разработка, корректировка и согласование организационно-распорядительных документов, планов, отчетов; обучение сотрудников);

- контрольные мероприятия (оценка достаточности применяемых мер и средств защиты информации; эффективность принимаемых мер; участие в работе контролирующих органов).

8. ПОРЯДОК РАЗРАБОТКИ, ВВОДА В ДЕЙСТВИЕ И ЭКСПЛУАТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Порядок, методы и способы обеспечения безопасности ПДн определяются руководящими и нормативно-методическими документами ФСТЭК и ФСБ России.

Безопасность ПДн при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных (далее – СЗПДн), включающей организационные меры и средства защиты информации (в том числе шифровальные средства, средства предотвращения несанкционированного доступа), а также используемые в системе информационные технологии.

Технические и программные средства, используемые для обработки ПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Средства защиты информации, применяемые в автоматизированных информационных системах, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

Основными стадиями создания СЗПДн являются:

- предпроектная, включающая предпроектное обследование и разработку технического задания на создание СЗПДн;

- проектирования, включающая разработку проекта на СЗПДн в составе объекта информатизации;

- ввода в действие СЗПДн, включающая опытную эксплуатацию и приёмо-сдаточные испытания, а также аттестацию объектов информатизации на соответствие требованиям безопасности информации.

Эксплуатация автоматизированных информационных систем и средств защиты информации в её составе осуществляется в соответствии с технологическим процессом и инструкциями по эксплуатации данных средств.

Для обеспечения безопасности ПДн при эксплуатации автоматизированных информационных систем и средств защиты информации необходимо соблюдать следующие требования:

- доступ к защищаемой информации лиц, работающих в автоматизированных информационных систем (пользователей, обслуживающего персонала), должен производиться в соответствии с порядком, установленным пунктом 3.3 настоящей Политики;

- на период обработки ПДн в помещениях, где размещаются основные технические средства и системы, могут находиться только лица, допущенные к обрабатываемой информации в порядке, установленном пунктом 3.3 настоящей Политики. Допуск других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться в эти помещения только в присутствии ответственного за обеспечение безопасности ПДн;

- при размещении в одном помещении нескольких технических средств отображения информации должен быть исключен несанкционированный просмотр выводимых на них данных;

- в случае компрометации парольной информации сотрудники должны действовать в соответствии с должностными инструкциями.

Все носители ПДн на бумажной, магнитной, оптической (магнито-оптической) основе, используемые подразделениями в технологическом процессе обработки в автоматизированных информационных системах, подлежат учету в этих структурных подразделениях.

Временно не используемые учтенные носители информации должны храниться в специально оборудованных для этого местах, недоступных для посторонних лиц.

Должен осуществляться периодический контроль, который включает в себя:

- контроль выполнения организационных мероприятий по обеспечению безопасности ПДн;
- инструментальный контроль эффективности внедренных средств защиты информации.

Инструментальный контроль проводится не реже одного раза в три года с привлечением на договорной основе организаций, проводивших аттестацию соответствующих объектов или других организаций, имеющих лицензию на соответствующий вид деятельности.

Инструментальный контроль является обязательным (необязательным по согласованию с аттестационным центром):

- при вводе аттестованных рабочих мест в эксплуатацию;
- после установки, ремонта или замены средств защиты информации;
- при значительных изменениях условий эксплуатации объекта информатизации или размещения технических средств.

По результатам контроля составляется акт, в котором оценивается состояние уровня защищенности на объекте, указываются имеющиеся нарушения и сроки их устранения, дается заключение.

Результаты работ докладываются генеральному директору Компании, который утверждает представляемый акт.

В случае имеющихся серьезных нарушений, работы на объекте информатизации приостанавливаются до их устранения.

9. ПРАВА И ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ КОМПАНИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

Функциональные обязанности и права генерального директора Компании по обеспечению безопасности ПДн:

- определяет ответственных за обеспечение безопасности ПДн;
- утверждает документы по обеспечению безопасности ПДн;
- принимает решение о финансировании работ по обеспечению безопасности ПДн;
- принимает решение о прекращении работ в структурном подразделении, где были выявлены нарушения требований по обеспечению безопасности ПДн, а также о возобновлении работ после устранения нарушений.

Функциональные обязанности и права ответственного за обеспечение безопасности ПДн:

- осуществляет годовое планирование мероприятий по обеспечению безопасности ПДн в Компании и контроль за их выполнением;
- организует разработку и внедрение необходимых организационно-технических мероприятий;

- представляет на утверждение генеральному директору Компании документы по обеспечению безопасности ПДн, в том числе список лиц допускаемых к обработке ПДн;

- оценивает эффективность принимаемых мер по обеспечению безопасности ПДн и организует работы по устранению выявленных недостатков;

- докладывает генеральному директору Компании предложения по устранению недостатков по обеспечению безопасности ПДн, выявленных в структурных подразделениях Компании;

- выявляет нарушения в технологии обработки ПДн;

- проверяет правильность функционирования систем разграничения доступа и наличие средств защиты информации;

- осуществляет документальное оформление проводимых защитных мероприятий;

- оказывает методическую помощь структурным подразделениям Компании в организации и проведении работ по обеспечению безопасности ПДн.

Функциональные обязанности и права руководителей и сотрудников структурных подразделений Компании по обеспечению безопасности ПДн:

- организуют и проводят работы по обеспечению безопасности ПДн в своих структурных подразделениях и на объектах информатизации, находящихся у них в эксплуатации;

- предоставляют ответственному за обеспечение безопасности ПДн список сотрудников, которым необходим доступ к ПДн в рамках выполнения трудовых (служебных) обязанностей;

- предоставляют генеральному директору Компании согласованный с ответственным за обеспечение безопасности ПДн перечень планируемых и реализуемых работ по обеспечению безопасности ПДн;

- согласовывают с ответственным за обеспечение безопасности ПДн установку на объекте средств вычислительной техники и средств связи;

- осуществляют постоянный контроль за правильностью эксплуатации и эксплуатацию технических средств защиты информации в структурном подразделении.

- Сотрудники Компании имеют право:

- запрашивать и получать от структурных подразделений Компании сведения, справочные и другие материалы, необходимые для осуществления деятельности по обеспечению безопасности ПДн;

- принимать участие в совещаниях по вопросам обеспечения безопасности ПДн, входящим в их компетенцию (по решению руководителя структурного подразделения);

- участвовать в семинарах (конференциях и т.п.) на темы защиты ПДн в качестве слушателя;

- вносить руководству Компании предложения по совершенствованию деятельности по обеспечению безопасности ПДн.

10.ВНУТРЕННИЙ КОНТРОЛЬ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ПДН

Для обеспечения постоянной защиты информационных ресурсов ИСПДн в Компании должны проводиться периодические мероприятия по внутреннему контролю уровня защищенности ИСПДн.

В периодические мероприятия должны включаться следующие мероприятия:

- контроль знаний сотрудников Компании по вопросам защиты ПДн;
- проверка компонентов ИСПДн на уязвимости;
- периодическая проверка работоспособности и настроек средств защиты информации;
- анализ журналов событий безопасности.

В планы могут включаться и другие необходимые мероприятия обеспечивающие надлежащий уровень информационной безопасности.

11.ПОРЯДОК ПУБЛИКАЦИИ И ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ДОКУМЕНТУ

В соответствии пунктом 2 статьи 18.1. Федерального закона от 27.07.2006 г. № 152 «О персональных данных» настоящая Политика должно быть опубликовано или иным образом обеспечен неограниченный доступ к настоящей Политике.

Настоящая Политика должна быть опубликовано на официальном сайте Компании по адресу: http://open-broker.ru в Разделе «Раскрытие информации» в формате PDF.

Настоящий документ может быть отправлено по электронной почте в случае его запроса.

12.СООТНОШЕНИЕ ВРЕДА И ПРИНИМАЕМЫХ КОМПАНИИ МЕР

В соответствии пунктом 2 статьи 18.1. Федерального закона от 27.07.2006 г. № 152 «О персональных данных» в настоящем Положении содержится оценка соотношения вреда и принимаемых Компаниим мер по защите ПДн.

Перечень принимаемых Компаниим мер перечислен в разделах 4 – 11 настоящей Политики. К основным принимаемым мерам относятся:

1) назначение ответственного за организацию обработки персональных данных;
2) издание документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с Федеральным Законодательством;
4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных в соответствии с Федеральным Законодательством и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальными актами оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушений, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законодательством;

6) ознакомление сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Компании в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.

Возможный вред, причиняемый субъекту ПДн в случае нарушения безопасности ПДн в ИСПДн в соответствии с Частной моделью угроз определяется, как незначительный в виду как целей обработки ПДн, так и в соотношении с принимаемыми мерами.

13.НОРМАТИВНО-ПРАВОВЫЕ АКТЫ И МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ ПО ЗАЩИТЕ ПДН ПРИ ИХ ОБРАБОТКЕ В ИСПДН

При подготовке настоящей Политики использованы следующие нормативно-правовые акты и методические документы по защите персональных данных при их обработке в информационных системах персональных данных:

1) Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»;

2) Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

3) Постановление Правительства РФ от 01.11.2012 г. № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»;

4) Приказ ФСТЭК России от 18.02.2013 г. № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

5) Руководящий документ ФСТЭК России от 15 февраля 2008 г. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

6) Руководящий документ ФСТЭК России от 14 февраля 2008 г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

7) Руководящий документ Гостехкомиссии России т 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации».