УТВЕРЖДЕНА
приказом Управляющего
Акционерного общества
«Санкт-Петербургская
Валютная Биржа»
от 28.10.2021 № 147/21-п

ПОЛИТИКА ОРГАНИЗАЦИИ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ АКЦИОНЕРНОГО ОБЩЕСТВА «САНКТ-ПЕТЕРБУРГСКАЯ ВАЛЮТНАЯ БИРЖА»

Санкт-Петербург
2021 год

Содержание

1. Термины и сокращения

Понятия, используемые в настоящей Политике, применяются в значениях, определенных Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных».

1.1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

1.2. Автоматизированное рабочее место (АРМ) – совокупность оборудования (персональный компьютер, принтер и т.п.) и установленного на нем ПО, предоставляемых АО СПВБ Пользователю для работы и выполнения должностных обязанностей.

1.3. Администратор информационной безопасности - работник отдела информационной безопасности и электронного документооборота.

1.4. Биржа – Акционерное общество «Санкт-Петербургская Валютная Биржа».

1.5. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

1.6. Информационная безопасность (ИБ) – состояние защищённости интересов (целей) АО СПВБ в условиях угроз в информационной сфере.

1.7. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.8. Инцидент информационной безопасности – событие информационной безопасности нежелательного и/или неожиданного характера, обладающее потенциалом нарушения конфиденциальности, целостности, доступности информации АО СПВБ.

1.9. Иные персональные данные – это персональные данные, которые не являются специальными (касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных), биометрическими (которые характеризуют физиологические и биологические особенности человека,

на основании которых можно установить его личность) и общедоступными (полученные только из общедоступных источников персональных данных).

1.10. Категории персональных данных – подразделяются на: персональные данные, специальные, биометрические, иные.

1.11. Конфиденциальность персональных данных – это создание условий, не допускающих их распространение или предоставление третьим лицам без согласия субъекта персональных данных, за исключением случаев, определённых законодательством РФ и/или, когда ПДн относятся к обезличенным/общедоступным.

1.12. Корпоративная вычислительная сеть (КВС) – множество (совокупность) взаимосвязанных аппаратных и программных средств и технологий, предназначенных для обработки, передачи и хранения информации в электронном виде.

1.13. Материальные носители информации – это бумажные носители, несъемные магнитные (жесткие диски и т.д.), съемные магнитооптические (дискеты и т.д.), съемные оптические носители (CD/DVD и т.д.), а также съемные и несъемные носители на основе флеш-памяти.

1.14. Машинный носитель - носитель используемый для записи и хранения информации, обеспечивающий ее обработку на средствах вычислительной техники.

1.15. Несанкционированный доступ – доступ к информации, осуществляемый с нарушением правил разграничения доступа.

1.16. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

1.17. Обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя:

- блокирование;
- запись;
- извлечение;
- использование;

- накопление;
- обезличивание;
- передачу (распространение, предоставление, доступ);
- сбор;
- систематизацию;
- удаление;
- уничтожение.
- уточнение (обновление, изменение);
- хранение.

1.18. Обработка персональных данных, осуществляемая без использования средств автоматизации - это обработка персональных данных, содержащихся в информационной системе персональных данных, либо извлеченных из такой системы, которая осуществляется без использования средств автоматизации (неавтоматизированная обработка), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.19. Оператор персональных данных (Оператор) – Акционерное общество «Санкт-Петербургская Валютная Биржа» самостоятельно или совместно с другими лицами организующая и (или) осуществляющая обработку персональных данных, а также определяющая цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.20. Персональные данные – любая информация, относящаяся к прямо или косвенно определённому или определяемому лицу, субъекту персональных данных.

1.21. Политика организации работы с персональными данными Акционерного общества «Санкт-Петербургская Валютная Биржа» (далее Политика) – локальный нормативный акт, определяющий цели, принципы и положения обработки персональных данных, а также процедуры, направленные на предотвращение, выявление и устранение нарушений законодательства Российской Федерации в отношении обработки персональных данных.

1.22. Пользователь – работник (сотрудник) организации или представитель внешней стороны, использующий в своей деятельности информационные системы организации на любых законных основаниях.

1.23. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

1.24. Работник (сотрудник) – лицо, выполняющее свои функции согласно трудовому договору и должностной инструкции, или согласно договору гражданско-правового характера с Акционерным обществом «Санкт-Петербургская Валютная Биржа».

1.25. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

1.26. Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

1.27. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.28. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

1.29. Сокращения:

- АО СПВБ - Акционерное общество «Санкт-Петербургская Валютная Биржа»
- АРМ – автоматизированное рабочее место.
- БД – база данных.
- ИБ – информационная безопасность.
- ИР – информационные ресурсы.
- ИС – информационные системы.
- ИСПДн – информационная система персональных данных.
- ОИБиЭДО – отдел информационной безопасности и электронного документооборота.
- ПДн – персональные данные.
- ПО – программное обеспечение.
- РФ – Российская Федерация.
- СВТ – средства вычислительной техники.
- СЗПДн - средства защиты персональных данных.
- СУБД - система управления базой данных.

- УЦ – удостоверяющий центр.
- ФЗ – федеральный закон.

2. Общие положения

2.1. Политика организации работы с персональными данными АО СПВБ направлена (разработана) для обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, а также защиты прав на неприкосновенность его частной жизни, личной и семейной тайны.

2.2. Политика организации работы с персональными данными АО СПВБ определяет цели и положения (регламенты) обработки персональных данных, а также процедуры, направленные на предотвращение, выявление и устранение нарушений законодательства Российской Федерации в отношении организации работы с персональными данными, которыми должны руководствоваться все пользователи, обрабатывающие персональные данные в соответствии со своими должностными обязанностями.

2.3. Целью настоящей Политики является выполнение требований законодательства Российской Федерации в области обработки и защиты Персональных данных.

2.4. Политика распространяется на все основные, обеспечивающие и управляющие бизнес-процессы АО СПВБ, а также технологические процессы, подпроцессы, процедуры и операции, в рамках которых осуществляется Обработка Персональных данных.

2.5. Действие настоящей Политики не распространяется на отношения, возникающие при:

- Обработке ПДн физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов Персональных данных;
- Организации хранения, комплектования, учета и использования содержащих Персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- Обработке ПДн, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

2.6. Настоящая Политика не регулирует взаимоотношения в части применения положений Общего регламента Европейского союза о защите данных от 27.04.2016 № 2016/679 (GDPR) и стандартов Комитета по безопасности индустрии платежных карт (PCI SSC).

2.7. Настоящая Политика обязательна для применения всеми работниками АО СПВБ, независимо от занимаемой ими должности, включая руководство, а также посетителями/пользователями информационных ресурсов Биржи.

2.8. Настоящая Политика, а также все изменения и дополнения к ней принимаются и утверждаются в установленном в АО СПВБ порядке и действуют до замены их новыми.

2.9. Изменения в настоящую Политику могут вноситься в случаях изменения законодательства Российской Федерации о Персональных данных и принятых в соответствии с ним нормативных правовых актов, существенного изменения в структуре технологических и бизнес-процессов, в рамках которых осуществляется обработка ПДн, изменения организационной структуры, а также по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, по результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

2.10. В случае изменения законодательства Российской Федерации о Персональных данных и принятых в соответствии с ним нормативных правовых актов, изменения или введения в действие стандартов, нормативно-методических рекомендаций, требований уполномоченных органов настоящая Политика применяется в части, не противоречащей вновь принятым нормативным правовым документам.

2.11. Внутренние нормативные и распорядительные документы АО СПВБ, затрагивающие вопросы обработки и защиты Персональных данных, должны разрабатываться с учетом положений настоящей Политики и не противоречить им.

2.12. При разработке дополнительных внутренних нормативных документов по вопросам, касающимся обработки и защиты ПДн, такие акты не могут и не должны содержать положения, ограничивающие права субъектов ПДн, устанавливать не предусмотренные Федеральным законодательством ограничения деятельности

Оператора или возлагать на Оператора не предусмотренные федеральными законами обязанности.

2.13. Настоящая Политика является общедоступной и подлежит размещению на официальном сайте Биржи.

2.14. Лицо (пользователь, или работник Оператора), осуществляющий обработку ПДн по поручению оператора, не обязано получать согласие субъекта ПДн на обработку его ПДн.

2.15. Обработка Оператором специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и/или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных федеральным законом «О персональных данных».

2.16. Настоящая Политика разработана в соответствии с требованиями:

- Конституции РФ (ст. 23, 24);
- Гражданского кодекса РФ (ст. 152.2);
- Трудового кодекса РФ;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федерального закона от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 29.07.2004 года № 98-ФЗ «О коммерческой тайне»;
- ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер;
- Постановления Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных

при их обработке в информационных системах персональных данных»;

- Положения Банка России от 20.04.2021 N 757-П "Об установлении обязательных для не кредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций";
- Приказа 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»;
- Приказа Роскомнадзора от 24.02.2021 N 18 "Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения" (Зарегистрировано в Минюсте России 21.04.2021 N 63204);
- Рекомендаций Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31.07.2017 «Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом «О персональных данных»;
- Политики информационной безопасности АО СПВБ.

2.17. Права субъекта персональных данных. Субъект ПДн имеет право на:

- Доступ к своим ПДн;
- Получение полной информации, касающейся обработки его ПДн, в том числе содержащей:
    1. подтверждение факта обработки персональных данных оператором;
    2. правовые основания и цели обработки персональных данных;
    3. цели и применяемые оператором способы обработки персональных данных;

4. наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона;
5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
6. сроки обработки персональных данных, в том числе сроки их хранения;
7. порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
8. информацию об осуществленной или о предполагаемой трансграничной передаче данных;
9. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
10. иные сведения, предусмотренные Федеральным законодательством.

– Предварительное согласие при обработке персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации. Указанная обработка персональных данных признается осуществляемой без предварительного согласия субъекта персональных данных, если оператор не докажет, что такое согласие было получено, в таком случае оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных;
– Возможность заявить возражение против решения, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные

интересы, которое может быть принято на основании исключительно автоматизированной обработки его персональных данных, которое не может приниматься без согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных;

- Обжалование действий или бездействий оператора в случае если субъект ПДн считает, что оператор осуществляет обработку его ПДн с нарушением требований федерального законодательства или иным образом нарушает его права и свободы, в уполномоченном органе по защите прав субъектов ПДн или в судебном порядке, в том числе и на возмещение убытков и (или) компенсацию морального вреда.

2.18. Оператор персональных данных при обработке ПДн обязан:

2.19.1. Предоставить субъекту персональных данных по его просьбе и в соответствии с его правами, информацию, касающеюся обработки его персональных данных;

2.19.2. Разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные если предоставление персональных данных является обязательным в соответствии с федеральным законом;

2.19.3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, когда оператор в соответствии с законодательством освобождается от обязанности предоставить такие сведения, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;

- установленные настоящим Федеральным законом права субъекта персональных данных;
- источник получения персональных данных.

2.19.4. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных федеральным законодательством.

2.19.5. Соблюдать конфиденциальность ПДн, а именно, не раскрывать третьим лицам и не распространять ПДн субъекта, без его согласия, если иное не предусмотрено Федеральным законом.

2.19.6. Обеспечить защиту и информационную безопасность обрабатываемых ПДн от несанкционированного доступа и разглашения, неправомерного использования или утраты;

2.19.7. Принимать необходимые и достаточные меры для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»:

- Назначить лицо ответственное за организацию обработки персональных данных;
- Назначить лицо, ответственное за обеспечение безопасности персональных данных в ИСПДн АО СПВБ;
- Издать необходимые и достаточные документы, реализующие настоящую Политику, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- Применить правовые, организационные и технические меры по обеспечению защиты и безопасности персональных данных;

- Осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному законодательству, нормативным правовым актам, требованиям к защите персональных данных, Политике оператора в отношении обработки персональных данных, локальным актам Оператора;
- Производить регулярную, не реже одного раза в год, оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального законодательства, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;

2.19.8. Ознакомить новых работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки и защиты персональных данных, и при необходимости провести их обучение;

2.19.9. Опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему Политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

2.19. Оператор по запросу уполномоченного органа по защите прав субъектов персональных данных обязан представить документы и локальные акты, подтверждающие принятие мер по защите ПДн.

2.20. В случае изменения законодательства Российской Федерации, нормативных или распорядительных документов АО СПВБ, затрагивающих действие настоящей Политики, положения Политики применяются в части, не противоречащей данным изменениям.

3. Цели обработки персональных данных

3.1. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.2. Обработка ПДн Биржей осуществляется в следующих целях:

3.2.1. Осуществления деятельности АО СПВБ;

3.2.2. Организации и ведения бухгалтерского и налогового учета;

3.2.3. Организации и ведения кадрового учета работников Биржи;

3.2.4. Исполнения обязательств, предусмотренных локальными нормативными актами и договорами (в т.ч. трудовыми);

3.2.5. Исполнения обязательств, предусмотренных федеральным законодательством и иными нормативными правовыми актами (в том числе в области охраны труда, промышленной безопасности и охраны окружающей среды);

3.2.6. Содействия работникам в обучении и карьерном росте;

3.2.7. Обязательного и добровольного страхования работников;

3.2.8. Повышения квалификации и обучения работников;

3.2.9. Обеспечения соответствия требованиям законодательства Российской Федерации в связи с осуществлением профессиональной деятельности;

3.2.10. Выплаты денежных средств работникам в связи с осуществлением ими трудовой деятельности;

3.2.11. Выполнения требований по пенсионному обеспечению работников;

3.2.12. Содействия в получении социальных льгот и компенсаций для работников и членов их семей;

3.2.13. Наделения работников полномочиями по заключению сделок и совершению иных действий от имени АО СПВБ;

3.2.14. Организации идентификации и учета контрагентов, обеспечения договорных правоотношений АО СПВБ, а также организации бухгалтерского учета АО СПВБ;

3.2.15. Осуществления возложенной на АО СПВБ обязанности по ведению списка инсайдеров в соответствии с Федеральным законом от 27 июля 2010 года № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;

3.2.16. Организации управления АО СПВБ;

3.2.17. Осуществления деятельности удостоверяющего центра в соответствии с законодательством Российской Федерации об электронной подписи;

3.2.18. Рассмотрения резюме и подбора кандидатов на вакантные должности для дальнейшего трудоустройства;

3.2.19. Проведения внутренних проверок и служебных расследований;

3.2.20. Осуществления деловых контактов, и в иных законных целях.

4. Правовые основания обработки персональных данных

4.1. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми оператор осуществляет обработку персональных данных.

4.2. Правовыми основаниями обработки ПДн в АО СПВБ являются:

- Трудовой кодекс РФ от 30.12.2001 г. № 197-ФЗ;
- Налоговый кодекс РФ от 31.07.1998г. №146-ФЗ (часть первая), от 05.08.2000г. №117-ФЗ (часть вторая);

- Федеральный закон от 15.12.2001 г. № 167-ФЗ «Об обязательном пенсионном страховании»;
- Федеральный закон от 29.11.2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федеральный закон от 01.04.1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Федеральным закон от 29.12.2006 г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;
- Гражданский кодекс РФ от 30.11.1994 г. №51-ФЗ (часть первая), от 26.01.1996 г. №14-ФЗ (часть вторая);
- Федеральный закон от 22.10.2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Федеральный закон от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах»;
- Федеральный закон от 7 февраля 2011 г. № 7-ФЗ «О клиринге, клиринговой деятельности и центральном контрагенте»;
- Федеральный закон от 27 июля 2010 года № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;
- Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции»;
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 28.03.1998 г. № 53-ФЗ «О воинской обязанности и военной службе»;
- Устав и иные нормативные акты АО СПВБ, согласия субъектов персональных данных.

5. Объём и категории обрабатываемых персональных данных, категории субъектов персональных данных

5.1. Объём и содержание обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

5.2. Категории обрабатываемых персональных данных:

5.2.1. Фамилия, имя, отчество;

5.2.2. Год, месяц и дата рождения;

5.2.3. Место и адрес рождения;

5.2.4. Адрес регистрации и проживания;

5.2.5. Семейное положение, образование, профессия, доходы;

5.2.6. Сведения об обязательном и добровольном страховании работников;

5.2.7. Сведения об изменении фамилии, количество детей в возрасте до 18 лет;

5.2.8. Паспортные данные;

5.2.9. Трудовой стаж;

5.2.10. СНИЛС;

5.2.11. ИНН;

5.2.12. Данные о предыдущих работодателях;

5.2.13. Номер расчетного счета;

5.2.14. Гражданство, занимаемые должности за последние 5 лет;

5.2.15. Должности в органах управления других юридических лиц.

5.3. Категории субъектов, персональные данные которых обрабатываются:

5.3.1. Кандидаты на вакантные должности АО СПВБ;

5.3.2. Работники и бывшие работники АО СПВБ;

5.3.3. Родственники работников АО СПВБ;

5.3.4. Кандидаты в члены органов управления и контроля АО СПВБ;

5.3.5. Физические лица входящие в органы управления и контроля АО СПВБ;

5.3.6. Работники заявители на создание сертификата ключа проверки электронной подписи;

5.3.7. Представители юридических лиц — контрагентов и потенциальных контрагентов АО СПВБ;

5.3.8. Физические лица, оказывающие или оказавшие услуги АО СПВБ по договорам гражданско-правового характера (в том числе потенциальных исполнителей по договорам);

5.3.9. Физические лица, получившие доступ к инсайдерской информации АО СПВБ;

5.3.10. Физические лица, включенные в группу лиц АО СПВБ в соответствии с ФЗ «О защите конкуренции».

5.4. Согласно Приложению 1. "Перечень персональных данных, обрабатываемых в АО СПВБ" утверждены обрабатываемые в АО СПВБ персональные данные.

6. Порядок и условия обработки персональных данных

6.1. Обработке подлежат только ПДн, которые отвечают целям их обработки.

6.2. При обработке ПДн не допускается:

- объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, не совместимых между собой;
- обработка ПДн, несовместимая с целями сбора персональных данных.

6.3. Обработка ПДн осуществляется:

- с согласия субъекта персональных данных на их обработку, составленного в письменном виде;
- в случаях, когда обработка ПДн необходима для осуществления и выполнения, возложенных законодательством Российской Федерации функций, полномочий и обязанностей для осуществления деятельности АО СПВБ;
- в случаях, когда осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн либо по его просьбе (далее – общедоступные ПДн).

6.4. В случае обработки ПДн с согласия субъекта ПДн такое согласие подписывается субъектом ПДн собственноручно либо его уполномоченным представителем. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». В случае если согласие на обработку ПДн дается представителем субъекта ПДн от лица субъекта ПДн, Биржа осуществляет проверку полномочий представителя. Согласие на обработку ПДн может быть отозвано субъектом ПДн в порядке, предусмотренном законодательством Российской Федерации.

6.5. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъектом персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

6.6. При заключении оператором договоров с третьими лицами, когда характер взаимодействия предполагает поручение обработки ПДн, в обязательном порядке контролировать их содержание в части: перечня действий (операций) с ПДн, которые будут совершаться третьим лицом, осуществляющим обработку ПДн по поручению АО СПВБ; цели обработки ПДн; обязанности третьего лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке; требований к защите обрабатываемых ПДн (в соответствии со статьёй 19 Федерального закона «О персональных данных»). Если в содержании этих договоров нет указанных требований, то принимается решение о необходимости их пересмотра или заключению дополнительного соглашения об условиях поручения обработки ПДн и обеспечению их безопасности.

6.7. Все договоры с третьими лицами, которые предполагают поручение обработки ПДн, в обязательном порядке должны согласовываться с ОИБиЭДО.

6.8. Хранение персональных данных рекомендуется осуществлять в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором, стороной

которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.9. При осуществлении хранения персональных данных оператор персональных данных обязан использовать базы данных, находящиеся на территории Российской Федерации.

6.10. Рекомендуется указывать иные условия хранения персональных данных, в том числе, при обработке персональных данных без использования средств автоматизации.

6.11. Рекомендуется указывать сроки хранения персональных данных.

6.12. Устанавливаются следующие сроки обработки и хранения персональных данных:

- персональные данные, обрабатываемые в целях основной деятельности, - в течение срока действия гражданско-правового договора и срока исковой давности после его завершения;
- персональные данные, обрабатываемые в связи с трудовыми отношениями, — в течение действия трудового договора и 75 лет после завершения действия трудового договора;
- персональные данные кандидатов на вакантные должности, в том числе и тех, кто не был оформлен на работу, - действуют до момента заключения трудового договора или получения субъектом персональных данных извещения (уведомления) об отказе в приеме на работу.

6.13. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации.

6.13.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (на полях бланков).

6.13.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не

совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6.13.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

6.13.4. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

– необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения

подлинности персональных данных, сообщенных субъектом персональных данных;

- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

6.13.5. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

6.13.6. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных

данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

6.13.7. Правила, предусмотренные пунктами 6.13.6 и 6.13.7. настоящей Политики, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

6.13.8. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

7. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите информации

7.1. Служба внутреннего контроля Биржи осуществляет мониторинг системы внутреннего контроля Оператора, проводит текущие и плановые проверки в части соблюдения требований регуляторного риска.

7.2. Служба внутреннего аудита Биржи осуществляет контроль за исполнением требований законодательства в части защиты персональных данных при проведении плановых и внеплановых проверок, а также проверку эффективности организации работы по данному направлению деятельности.

7.3. Внутренний контроль соответствия обработки ПДн установленным требованиям осуществляется путем проведения плановых и внеплановых проверок условий обработки ПДн (далее – проверка) на основании плана осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн,

определяющего цель и срок проведения проверки, утвержденного единоличным исполнительным органом Биржи - Управляющим.

7.4. Проверка осуществляется ответственным за организацию обработки ПДн в комиссии, либо комиссией по контролю соответствия обработки ПДн требованиям к защите ПДн на Бирже, состав которой утверждается единоличным исполнительным органом Биржи - Управляющим. Количественный состав комиссии не должен быть менее трех членов (председатель и 2 члена). Лицо, ответственное за организацию ПДн, в состав комиссии не входит. В проведении проверки не может участвовать сотрудник Биржи, прямо или косвенно заинтересованный в ее результатах.

7.5. Плановые проверки проводятся не чаще чем один раз в два года.

7.6. В случае поступившего на Биржу письменного заявления субъекта ПДн о нарушениях правил обработки ПДн проводится внеплановая проверка. Проведение внеплановой проверки организуется в течение 3 рабочих дней с момента поступления соответствующего заявления.

7.7. При проведении проверки соответствия обработки ПДн установленным требованиям к защите персональных данных должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн АО СПВБ;
- состояние учета машинных носителей ПДн;
- соблюдение правил доступа к ПДн;
- наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;
- мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности ПДн.

7.8. В ходе проведения внутреннего контроля лицо, ответственное за организацию обработки ПДн, и комиссия, должны обеспечивать конфиденциальность персональных данных.

7.9. Проверка должна быть завершена не позднее чем через 20 календарных дней со дня принятия решения о ее проведении.

7.10. По результатам проверки, проведенной комиссией, непосредственно после ее завершения в двух экземплярах составляется акт, который подписывается всеми членами комиссии и согласуется с лицом, ответственным за организацию обработки ПДн. Один экземпляр указанного акта представляется единоличному исполнительному органу Биржи – Управляющему, другой хранится у лица, ответственного за организацию обработки ПДн.

8. Защита персональных данных и обеспечение информационной безопасности при их обработке

8.1. АО СПВБ для обеспечения безопасности и защиты Персональных данных принимает правовые, организационные и технические меры от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн.

8.2. Все внутренние нормативные и распорядительные документы АО СПВБ, затрагивающие вопросы обработки и защиты Персональных данных, подлежат обязательному согласованию с ответственным за организацию Обработки Персональных данных и ответственным подразделение за обеспечение безопасности Персональных данных - Отделом информационной безопасности и электронного документооборота.

8.3. Мероприятия по защите и обеспечению безопасности ПДн являются составной частью деятельности АО СПВБ по защите конфиденциальной (защищаемой) информации.

8.4. Ответственными за реализацию и организацию выполнения требований Политики и внутренних нормативных документов Биржи по вопросам обработки ПДн и их защите в структурных подразделениях являются руководители

подразделений. На время отсутствия руководителей ответственными являются лица, замещающие их. Руководители подразделений вправе назначить иных должностных лиц ответственными по отдельным вопросам организации обработки и защиты ПДн.

8.5. Руководители подразделений обязаны:

- осуществлять контроль за соблюдением подчинёнными работниками требований законодательства РФ об обработке и защите ПДн;
- доводить до сведения подчинённых работников положения законодательства РФ о ПДн, внутренних нормативных документов по вопросам обработки ПДн, требований к защите ПДн;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приёмом и обработкой таких обращений и запросов.
- организовывать выполнение законодательных требований при обработке ПДн подчинёнными работниками.

8.6. Работники АО СПВБ, допущенные (уполномоченные в установленном порядке) обрабатывать ПДн, обязаны выполнять требования Федерального законодательства и внутренних нормативных документов Биржи по вопросам обработки ПДн и их защите на своих рабочих местах.

8.7. Доступ к настройкам средств защиты информации в ИСПДн разрешён только работникам отдела информационной безопасности, в рамках поставленных перед отделом задач. Доступ к настройкам фиксируется в электронных журналах программных и программно-технических компонент ИСПДн.

8.8. Выполнение процедур резервного копирования информации, содержащей ПДн определяется документом, регламентирующим порядок резервного копирования информации.

8.9. Серверные компоненты ИСПДн расположены в периметре охраняемого помещения. Физический доступ к серверам ограничен перечнем лиц, имеющих доступ к серверному оборудованию.

8.10. АРМ пользователей, на которых производится обработка ПДн находятся в помещениях, оборудованных системами контроля доступа и защищены круглосуточным постом физической охраны.

8.11. Технические средства, предназначенные для администрирования ИСПДн, серверные компоненты ИСПДн и автоматизированные рабочие места пользователей находятся в разных сегментах локальной вычислительной сети.

8.12. Мониторинг трафика осуществляется средствами межсетевого экранирования. Мониторинг проводится отделом информационной безопасности на регулярной основе.

8.13. Все съемные носители и накопители информации перед использованием должны быть проверены работниками отдела информационной безопасности, на наличие вредоносных программ и возможных угроз безопасности.

8.14. Коммуникационные порты и устройства ввода вывода на АРМ пользователей где обрабатываются ПДн функционируют, обеспечивая минимальный необходимый набор возможностей для выполнения служебных задач.

8.15. Мониторинг информационного взаимодействия между сегментами локальной вычислительной сети, и защита сегментов локальной вычислительной сети осуществляется сертифицированными по требованиям безопасности информации программно-аппаратными техническими средствами защиты, в соответствии с требованиями приказа ФСТЭК от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных». Администрирование средств защиты информации осуществляет отдел информационной безопасности.

8.16. Доступ к информации, содержащей ПДн на электронных носителях (сервера баз данных, пользовательские и клиентские АРМ) ограничен реализацией следующих мер защиты ИСПДн:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- защитой машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн;
- регистрацией событий безопасности;
- антивирусной защитой;
- контролем (анализом) защищенности ПДн;
- обеспечением целостности информационной системы и ПДн;

- обеспечение доступности ПДн;
- защитой технических средств;
- защитой информационной системы, ее средств, систем связи и передачи данных;
- выявлением инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности ПДн и реагированию на них;
- управление конфигурацией информационной системы и системы защиты ПДн;
- защитой информации при ее передаче по каналам связи, выходящим за пределы контролируемой зоны;
- организацией физической защиты помещений и технических средств обработки ПДн;
- разграничением доступа пользователей к программным средствам обработки ПДн и средствам защиты ПДн;
- резервированием технических средств и массивов ПДн;
- использованием средств межсетевого экранирования при взаимодействии ИСПДн с сетью международного информационного обмена (Интернет).

8.17. Безопасность ПДн, обработка которых осуществляется без использования средств автоматизации, достигается реализацией следующих мер безопасности:

8.18.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

8.18.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей с персональными данными), обработка которых осуществляется в различных целях.

8.18.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

8.18. Хранение ПДн должно исключать их утрату или несанкционированный доступ к ним.

8.19. Документы, содержащие ПДн, хранятся в помещениях подразделений, ответственных за ведение и хранение таких документов. Входные двери помещений оборудуются замками, гарантирующими надёжное закрытие помещений во внерабочее время, и оснащаются охранно-пожарной сигнализацией.

8.20. Оператор обеспечивает хранение первичных документов, связанных с обработкой документации по учёту кадров, учёту использования рабочего времени, оплаты труда. Документы на бумажных носителях, содержащие ПДн работников, с которыми расторгнуты трудовые отношения, сдаются в архив.

8.21. Настоящей Политикой утвержден перечень информации, технических средств и объектов, подлежащих защите в ИС ПДн АО СПВБ "Приложение 2. Перечень информации, технических средств и объектов, подлежащих защите в информационных системах персональных данных АО СПВБ".

9. Актуализация, исправления, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

9.1. При выявлении неправомерной обработки ПДн при обращении субъекта персональных данных или его представителя, либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных, осуществляется блокирование неправомерно обрабатываемых Персональных данных, относящихся к этому субъекту ПДн, или обеспечивается их блокирование (если Обработка Персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. Обращения субъектов ПДн учитываются в журнале учета обращений субъектов персональных данных.

9.2. В случае подтверждения факта неточности Персональных данных Оператор на основании сведений, представленных субъектом Персональных данных или его представителем (или иных необходимых документов), обязан уточнить ПДн, либо обеспечить их уточнение (если Обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять Блокирование Персональных данных.

9.3. В случае выявления неправомерной Обработки Персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную Обработку Персональных данных или обеспечить прекращение неправомерной Обработки Персональных данных лицом, действующим по поручению Оператора.

9.4. В случае если обеспечить правомерность Обработки Персональных данных невозможно, Оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной Обработки Персональных данных, обязан уничтожить такие Персональные данные или обеспечить их Уничтожение.

9.5. Об устранении допущенных нарушений или об Уничтожении Персональных данных Оператор обязан уведомить субъекта Персональных данных или его представителя, а в случае, если обращение субъекта Персональных данных или его представителя, либо запрос уполномоченного органа по защите прав субъектов Персональных данных были направлены уполномоченным органом по защите прав субъектов Персональных данных, также в указанный орган.

9.6. В случае достижения цели Обработки Персональных данных Оператор обязан прекратить Обработку Персональных данных или обеспечить ее прекращение (если Обработка Персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить Персональные данные или обеспечить их Уничтожение (если Обработка Персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Оператором и субъектом Персональных данных, либо если Оператор не вправе

осуществлять Обработку Персональных данных без согласия субъекта Персональных данных на основаниях, предусмотренных Федеральными законами.

9.7. В случае отзыва субъектом Персональных данных согласия на обработку ПДн Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если Обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и в случае если сохранение Персональных данных более не требуется для целей Обработки Персональных данных уничтожить Персональные данные или обеспечить их Уничтожение (если Обработка Персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект Персональных данных, иным соглашением между Оператором и субъектом Персональных данных, либо если Оператор не вправе осуществлять Обработку Персональных данных без согласия субъекта Персональных данных на основаниях, предусмотренных федеральными законами.

9.8. В случае отсутствия возможности уничтожения ПДн в течение установленного срока, Оператор осуществляет Блокирование таких Персональных данных или обеспечивает их Блокирование (если Обработка Персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

9.9. Оператор обязан прекратить обработку ПДн, разрешенных для распространения, в течение трех рабочих дней с момента получения письменного требования работника Оператора или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

9.10. В случае предоставления субъектом персональных данных заявления на исключение или исправление неверных или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для АО СПВБ персональных данных, фактов о неполных, устаревших, недостоверных или незаконно полученных персональных данных Оператор должен внести

необходимые изменения, уничтожить или блокировать их, а также уведомить о своих действиях субъекта персональных данных.

9.11. В случае подтверждения факта неточности в персональных данных они подлежат актуализации оператором, а при неправомерности их обработки такая обработка должна быть прекращена.

9.12. Когда цели обработки ПДн достигнуты или субъект ПДн отозвал свое согласие, персональные данные должны быть уничтожены, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;
- оператор не вправе осуществлять обработку без согласия субъекта ПД на основаниях, предусмотренных Законом о ПД или иными федеральными законами;
- иное не предусмотрено иным соглашением между оператором и субъектом ПДн.

9.13. По запросу субъекта персональных данных (его представителя) Оператор обязуется сообщить о наличии у него его персональных данных, а также предоставить возможность ознакомления с ними.

10. Учет, использование, хранение и уничтожение материальных носителей данных, предназначенных для обработки и хранения персональных данных

10.1. Все носители персональных данных, используемые при работе со средствами вычислительной техники (СВТ) для обработки и хранения персональных данных, в обязательном порядке регистрируются и учитываются.

10.2. Ответственность за организацию учета и использования носителей данных, предназначенных для обработки и хранения персональных данных, возлагается на сотрудника, отвечающего за организацию обработки персональных данных.

10.3. Персональную ответственность за сохранность полученных из машинных носителей данных и предотвращение несанкционированного доступа к записанной на них ПДн несет сотрудник АО СПВБ, получивший эти носители в целях исполнения служебных обязанностей.

10.4. Машинные носители информации, содержащие ПДн, учитываются в журнале учета носителей персональных данных.

10.5. Несъемные машинные носители персональных данных закрепляются за сотрудником, ответственным за СВТ, входящие в состав АРМ пользователей и серверов, в котором они установлены.

10.6. Хранение носителей персональных данных осуществляется в тех подразделениях Организации, где они используются, если иное не установлено приказами руководства Биржи. Хранение персональных данных субъектов ПДн осуществляют сотрудники, которые имеют право доступа к персональным данным, в порядке, исключающем доступ к ним третьих лиц.

10.7. Подразделения АО СПВБ, хранящие архивные ПДн на бумажных носителях, обязаны обеспечить ограничение доступа к указанным данным и допустить к ним только тех сотрудников, деятельность которых непосредственно связана с обработкой хранимого типа архивных ПДн.

10.8. Персональные данные сотрудников АО СПВБ хранятся в личных делах сотрудников в Отделе кадрового и документационного обеспечения. Личные дела работников хранятся в бумажном виде в папках и находятся в сейфе или в металлическом шкафу.

10.9. Персональные данные субъектов ПДн хранятся в соответствующих подразделениях АО СПВБ, которые отвечают за взаимодействие с субъектами ПДн.

10.10. Персональные данные субъектов ПДн Оператора хранятся также в электронном виде в ИСПДн. Доступ к электронным базам данных, содержащим персональные данные, обеспечивается с применением организационных и технических мер.

10.11. Работник АО СПВБ, имеющий доступ к персональным данным субъектов ПДн в связи с исполнением трудовых обязанностей, обеспечивает хранение информации, содержащей персональные данные, исключающее доступ к

ним третьих лиц. В отсутствие сотрудника на его рабочем месте не должно быть в открытом доступе носителей, содержащих персональные данные.

10.12. Копирование информации, составляющей персональные данные, с машинных носителей производится с разрешения сотрудника, ответственного за организацию обработки персональных данных по заявке руководителя структурного подразделения.

10.13. Уничтожение бумажных носителей, содержащих ПДн, осуществляется механическим путем с помощью специальных технических средств (шредеров, уничтожителей бумаг) о чем составляется соответствующий акт.

10.14. Передача материальных носителей, содержащих ПДн, третьим лицам (включая надзорные органы) возможна только в случаях, прямо предусмотренных законодательными и нормативными актами, либо в случае согласия субъекта ПДн. Факт передачи должен быть оформлен соответствующим актом.

10.15. При убытии в отпуск, служебную командировку и в иных случаях длительного отсутствия сотрудника на своем рабочем месте, он обязан передать носители, содержащие персональные данные, лицу, на которое по приказом (распоряжением) будет возложено исполнение его обязанностей. В случае если такое лицо не назначено, то документы и иные носители, содержащие персональные данные, передаются другому сотруднику, имеющему доступ к персональным данным по указанию руководителя структурного подразделения.

10.16. При увольнении сотрудника, имеющего доступ к персональным данным, документы и иные носители, содержащие персональные данные, передаются другому сотруднику, имеющему доступ к персональным данным по указанию руководителя структурного подразделения.

11. Обязанности и ответственность участников обработки и защиты персональных данных

11.1. Участниками процесса обработки и защиты ПДн Оператора являются:

- ответственный за организацию обработки ПДн;
- ответственный за обеспечение безопасности ПДн;
- лицо (работник Оператора) имеющий доступ к обработке ПДн.

11.2. Лицо, ответственное за организацию Обработки Персональных данных, назначается приказом Управляющего АО СПВБ.

11.3. В функции лица, ответственного за организацию Обработки Персональных данных, входят:

11.3.1. знание и неукоснительное соблюдение положений законодательства Российской Федерации, настоящей Политики, внутренних нормативных документов Биржи в области Обработки Персональных данных;

11.3.2. организация контроля за соблюдением Биржей и её работниками законодательства Российской Федерации в области обработки Персональных данных, а также исполнения распорядительных и внутренних нормативных документов Биржи по организации обработки ПДн;

11.3.3. доведение до сведения работников Биржи положений законодательства Российской Федерации о Персональных данных, локальных актов по вопросам Обработки Персональных данных;

11.3.4. организация приема и обработки обращений и запросов субъектов Персональных данных или их представителей и/или осуществление контроля за приемом и обработкой таких обращений и запросов;

11.3.5. выполнение иных функций, предусмотренных для лица, ответственного за организацию Обработки Персональных данных, должностной инструкцией.

11.4. Лицо, ответственное за обеспечение безопасности Персональных данных, назначается приказом Управляющего АО СПВБ.

11.5. В функции лица, ответственного за обеспечение безопасности ПДн при их обработке входят:

11.5.1. знание и неукоснительное соблюдение положений законодательства Российской Федерации, настоящей Политики, внутренних нормативных документов АО СПВБ в области защиты Персональных данных;

11.5.2. мониторинг выполнения работниками Оператора законодательства Российской Федерации в области обеспечения безопасности

Персональных данных, а также контроля исполнения распорядительных и внутренних нормативных документов Биржи по обеспечению безопасности Персональных данных;

11.5.3. организация контроля обеспечения уровня защищенности Персональных данных и эффективности принятых мер защиты Персональных данных при их Обработке;

11.5.4. рассмотрение и утверждение предложений по устранению недостатков и предупреждению нарушений при обеспечении безопасности Персональных данных, осуществление контроля устранения нарушений;

11.5.5. рассмотрение и утверждение предложений по совершенствованию системы безопасности Персональных данных;

11.5.6. выполнение иных функций, предусмотренных для лица, ответственного за обеспечение безопасности Персональных данных, должностной инструкцией.

11.6. Лицо, имеющее доступ к Обработке Персональных данных, обязан выполнять следующие функции:

11.6.1. знать и неукоснительно выполнять требования законодательства Российской Федерации о Персональных данных, настоящей Политики, внутренних нормативных документов Биржи, регламентирующих порядок обработки и защиты Персональных данных;

11.6.2. осознание актуальных угроз безопасности ПДн и принятие мер по предотвращению и преодолению их возможных последствий;

11.6.3. осуществлять обработку Персональных данных только в рамках выполнения своих должностных обязанностей;

11.6.4. не разглашать Персональных данных, полученных в результате выполнения своих должностных обязанностей, а также ставших ему известными по роду своей деятельности;

11.6.5. пресекать действий других лиц, которые могут привести к разглашению (уничтожению, искажению) Персональных данных;

11.6.6. выявлять факты разглашения (уничтожения, искажения) Персональных данных и информировать об этом своего непосредственного руководителя, ответственного за обработку ПДн и ответственного за безопасность ПДн;

11.6.7. выполнение иных функции, предусмотренных для лица, допущенного к Обработке Персональных данных, должностной инструкцией.

11.7. Также ответственность за организацию обработки ПДн субъектов персональных данных, возлагается и на руководителей подразделений, в которых обрабатываются ПДн, в соответствии с полномочиями, правами и обязанностями руководителей подразделений, определенных в должностных инструкциях и определённых настоящей Политикой.

11.8. Оператор при обработке ПДн обязан принимать необходимые правовые, организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

11.9. Ознакомление работников, принимаемых на работу со внутренними нормативными документами, а также нормативными актами и законодательством Российской Федерации в области безопасности ПДн, осуществляется ОИБиЭДО под подпись в «Журнале инструктажа по информационной безопасности» в соответствии с приказом «Об обучении и повышении осведомлённости по информационной безопасности работников в Акционерном обществе «Санкт-Петербургская Валютная Биржа».

11.10. Реализация запросов, обращений и требований субъектов ПДн осуществляется подразделением Оператора, непосредственно обслуживающим или взаимодействующим с субъектом персональных данных. Ответственность за уведомление субъекта ПДн, полноту, своевременность реализации и учёта выполнения мероприятий несёт руководитель данного подразделения.

11.11. Уведомление об обработке АО СПВБ ПДн, подготавливается и направляется в Роскомнадзор ответственным за организацию обработки персональных данных.

11.12. В случае изменения состава обрабатываемых ПДн, и/или иных сведений, содержащихся в уведомлении, ответственным за организацию обработки персональных данных в течение десяти рабочих дней, с даты внесения изменений, подготавливается и направляется в уполномоченный орган информационное письмо содержащее информацию о внесении изменений в уведомление об обработке ПДн.

11.13. Реализация запросов, обращений и требований уполномоченного органа по защите прав субъектов ПДн осуществляется ответственным за организацию обработки персональных данных АО СПВБ.

11.14. Работник, имеющий доступ к ПДн, виновный в нарушении порядка обращения с ПДн, несёт дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральным законодательством.

12. Заключительные положения

12.1. Требования, изложенные в Политике, являются обязательными для выполнения всеми работниками Биржи и иными лицами, имеющими договорные отношения с Оператором, при этом срочность и важность выполняемых ими работ не должны являться основанием для нарушения требований настоящей Политики.

12.2. Работники, непосредственно осуществляющие обработку ПДн, должны быть ознакомлены с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, документами Биржи, определяющими политику в отношении обработки ПДн, внутренними нормативными документами Биржи по вопросам обработки ПДн. С работниками, непосредственно осуществляющими обработку ПДн, должны быть в установленном порядке оформлены обязательства о выполнении требований внутренних нормативных актов Биржи по обработке, защите и неразглашении конфиденциальной информации, в том числе ПДн. Эти лица должны быть предупреждены о том, что обрабатываемые ими ПДн могут быть использованы лишь в целях, установленных законодательством РФ и внутренними нормативными актами Биржи, и они имеют право доступа только к тем ПДн, обработка которых предусмотрена должностными обязанностями (инструкциями).

Приложение 1.
Перечень персональных данных, обрабатываемых в АО СПВБ

Перечень персональных данных, обрабатываемых в АО СПВБ

№ п/п	Наименование (вид) ПДн	Содержание персональных данных	Источник получения	Основание обработки ПДн	Технологический процесс, использующий вид ПДн
1.	Сведения контрагентов, в том числе представителей контрагентов, необходимые для исполнения договорных обязательств и ведения бухгалтерского учета	- Фамилия, имя, отчество. - Паспортные данные: серия, номер, наименование органа, выдавшего его, дата выдачи. - Должность. - Гражданство. - СНИЛС. - ИНН. - Информация, содержащаяся в документах, дающих право на применение налоговых льгот.	- Субъект ПДн - Договор - Доверенность. - Федеральное законодательство - Государственные информационные ресурсы - Запросы в государственные органы, коммерческие организации.	- Законодательство РФ. - Согласие субъекта ПДн. - Условия договора.	- Заключение договора с контрагентом. - Изменение данных о контрагенте. - Прекращение или расторжение договора с контрагентом.
2.	Сведения сотрудников связи с реализацией трудовых отношений	- фамилия, имя, отчество, в том числе прежние фамилия, имя или отчество, а также дата, место и причина изменения; - паспортные данные: серия, номер, наименование органа, выдавшего его, дата выдачи;	- Субъект ПДн. - Трудовое законодательство. - Федеральное законодательство.	- Согласие субъекта ПДн. - Законодательство РФ. - Условия трудового договора.	- Передача в ЦБ РФ для согласования кандидатур на должности в соответствии с требованиями действующего законодательства.

		- число, месяц, год рождения; - место рождения; - гражданство; - сведения об образовании, в том числе наименование образовательной организации, год окончания обучения, наименование и реквизиты документов об образовании, квалификация, специальность; - сведения об ученой степени, ученом звании, в том числе дата присвоения, номер диплома, аттестата; - сведения о профессиональной переподготовке и/или повышении квалификации; - информация о наличии или отсутствии судимости; - сведения о выполняемой работе с начала трудовой деятельности; - сведения о занимаемых должностях в органах управления юридических лиц; - семейное положение, состав семьи; - сведения о воинском учете - место жительства, в том числе адрес места фактического проживания и адрес места регистрации; - номер расчетного счета; - номер банковской карты;	- Государственные информационные ресурсы. - Запросы в государственные органы, коммерческие организации.		- Заключение трудового договора. - Внесение изменений в трудовой договор. - Осуществление мероприятий по охране труда. - Оценка соответствия требованиям занимаемой должности. - Расторжение трудового договора. - Выдача справок.

		- реквизиты страхового свидетельства обязательного пенсионного страхования; - ИНН; - реквизиты полиса обязательного медицинского страхования; - информация, содержащаяся в свидетельствах о государственной регистрации актов гражданского состояния; - номер телефона (либо иной вид связи; - результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований); - сведения о доходах; - сведения из реестра - дисквалифицированных лиц; - сведения о выплате пенсий, пособий и иных социальных выплат; - информация, содержащаяся в документах, дающих право на применение налоговых льгот, а также влияющих на условия трудовых отношений.			
3.	Сведения в связи с осуществлением	- фамилия, имя, отчество, в том числе прежние фамилия, имя или	- Субъект ПДн.	- Согласие субъекта ПДн.	- Сбор предложений акционеров о

	деятельности и управления АО СПВБ	отчество, а также дата, место и причина изменения; - паспортные данные: серия, номер, наименование органа, выдавшего его, дата выдачи; - число, месяц, год рождения; - место рождения - гражданство; - сведения об образовании, в том числе наименование образовательной организации, год окончания обучения, наименование и реквизиты документов об образовании, квалификация, специальность; - сведения об ученой степени, ученом звании, в том числе дата присвоения, номер диплома, аттестата; - сведения о профессиональной переподготовке и/или повышении квалификации; - информация о наличии или отсутствии судимости; - сведения о выполняемой работе за последние 3 года; - сведения о занимаемых должностях в органах управления юридических лиц; - адрес места регистрации; - номер расчетного счета; - номер банковской карты;	- Оператор ПДн – акционер АО СПВБ.	- Предложение акционера/члена Совета директоров о выдвижении кандидата в орган управления. - Федеральное законодательство. - Государственные информационные ресурсы. - Запросы в государственные органы, коммерческие организации.	выдвижении кандидатов в органы управления. - Передача в ЦБ РФ для согласования кандидатур в члены Совета директоров. - Составление процедурных документов по деятельности органа управления. - Составление и раскрытие Годового отчета. - Раскрытие ПДн на официальном сайте в информационно-телекоммуникационной сети Интернет.

		- реквизиты страхового свидетельства обязательного пенсионного страхования; - ИНН; - номер телефона (либо иной вид связи; - сведения из реестра дисквалифицированных лиц.			
4.	Сведения в связи с включением в группу лиц с АО СПВБ	- фамилия, имя, отчество; - паспортные данные: серия, номер, наименование органа, выдавшего его, дата выдачи; - ИНН.	- Операторы ПДн, входящие в группу лиц с АО СПВБ; - Субъект ПДн.	- Согласие субъекта; - ФЗ «О защите конкуренции» № 135-ФЗ от 26.07.2006 г. (ст. 9)	- Составление отчетности в соответствии с требованиями ЦБ РФ - Передача отчетности в ЦБ РФ
5.	Сведения в связи с членством в Совете секций АО СПВБ	- фамилия, имя, отчество; - паспортные данные: серия, номер, наименование органа, выдавшего его, дата выдачи; - число, месяц, год рождения; - место рождения; - гражданство; - сведения об образовании, в том числе наименование образовательной организации, год окончания обучения, наименование и реквизиты документов об образовании, квалификация, специальность; - место работы;	- Субъект ПДн - Оператор (юр. л.), являющийся Участником торгов в какой-либо секции АО СПВБ	- Согласие субъекта ПДн	- Сбор предложений о выдвижении кандидатов в члены Совета секции; - передача в Совет директоров АО СПВБ для избрания состава Совета секции; - раскрытие ПДн на официальном сайте в информационно-телекоммуникационной сети Интернет; - составление процедурных документов по

		- должность; - номер телефона (либо иной вид связи).			деятельности Совета секций; - передача в ЦБ РФ в соответствии с ФЗ «Об организованных торгах» № 325-ФЗ от 21.11.11 г.
6.	Сведения в связи с соисканием кандидатов на вакантные должности в АО СПВБ	- фамилию, имя, отчество, год, месяц, дату и место рождения, - гражданство, адрес регистрации, адрес места жительства, - сведения, содержащиеся в документах, удостоверяющих личность, - сведения о семейном положении и составе семьи, - сведения об образовании, о владении иностранными языками, о наличии ученой степени, ученого звания, о научных трудах и изобретениях, - о занимаемой должности, данные о предыдущих местах работы, - сведения о доходах, - идентификационный номер налогоплательщика, номер страхового свидетельства обязательного пенсионного страхования, - сведения о воинском учете, данные о допуске к сведениям,	- Субъект ПДн - Государственные информационные ресурсы. - Запросы в государственные органы, коммерческие организации	- Согласие субъекта ПДн. - Федеральное законодательство.	Подбор персонала.

		составляющим государственную тайну, - сведения о наградах, - информацию о членстве в выборных органах, - сведения о социальных льготах, которые предоставляются в соответствии с законодательством и правовыми актами Российской Федерации, - фотографию, - телефонные абонентские номера (домашний, рабочий, мобильный), адрес электронной почты.			

Приложение 2.
Перечень информации, технических средств и объектов, подлежащих защите в информационных системах персональных данных АО СПВБ

1. Объектами защиты являются – информация, обрабатываемая в ИСПДн, технологическая информация ИСПДн, средства защиты ПДн, каналы программно-технические средства обработки ПДн, каналы информационного обмена и телекоммуникации, объекты и помещения, в которых размещены компоненты ИСПДн.
2. Объектами защиты каждой ИСПДн являются:
   2.1. Обрабатываемая информация:
   - персональные данные субъектов ПДн;
   - персональные данные сотрудников;

   2.2. Технологическая информация ИСПДн:
   - управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
   - технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
   - информация на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
   - информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;
   - информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
   - служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

   2.3. Программно-технические средства обработки ПДн:
   - общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);
   - резервные копии общесистемного программного обеспечения;
   - инструментальные средства и утилиты систем управления ресурсами ИСПДн;
   - аппаратные средства обработки ПДн (АРМ и сервера);
   - сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

2.4. Средства защиты ПДн, к которым относятся:
- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты ПДн, при их передачи.

2.5. Каналы информационного обмена и телекоммуникации:
- Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемые ПДн и технологическая информация.

2.6. Объекты и помещения, в которых размещены компоненты ИСПДн:
- Объекты и помещения являются объектами защиты, если в них происходит обработка ПДн и технологической информации, установлены технические средства обработки и защиты.