УТВЕРЖДАЮ

Директор

ООО «Ломбард «Выручка»

_____ Н.М.Пучинина

"01" сентября 2022г.

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ, КЛИЕНТОВ И КОНТРАГЕНТОВ

Общества с ограниченной ответственностью «Ломбард «Выручка»

(ООО «Ломбард «Выручка»)

Настоящее Положение разработано в соответствии с Конституцией РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данным», Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информатизации, информационных технологиях и защите информации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иными нормативными актами, действующими на территории Российской Федерации.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Целью настоящего Положения является защита персональных данных работников, клиентов и контрагентов Общества с ограниченной ответственностью «Народный ломбард» (далее - Общество) от несанкционированного доступа, неправомерного их использования или утраты.

1.2. В настоящем Положении используются следующие термины и определения:

Оператор – ООО «Ломбард «Выручка» (далее - Общество), вступившее в договорные отношения с работником, клиентом или контрагентом или оказывающее услуги физическому лицу, юридическому лицу или индивидуальному предпринимателю.

Клиент – физическое лицо, представитель - физическое лицо юридического лица или индивидуального предпринимателя, вступившее в договорные отношения по оказанию услуг с Обществом.

Контрагент – физическое лицо, представитель – физическое лицо юридического лица и индивидуального предпринимателя, вступившее с Обществом в договорные отношения.

Персональные данные Клиента – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Клиента, в том числе: фамилия, имя, отчество, полная дата рождения, место рождения, адрес проживания и регистрации, семейное положение, образование, профессия, специальность, место работы, занимаемая должность по месту работы, размер получаемых доходов от трудовой деятельности, ИНН, сведения ВУС, СНИЛС, сведения об общем и трудовом стаже, адрес электронной почты, номер телефона, место работы или учебы членов семьи и близких родственников, состав декларируемых сведений о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию, налоговый статус (резидент/нерезидент), иные сведения, указанные заявителем.

Персональные данные Контрагента – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Контрагента, в том числе: фамилия, имя, отчество, полная дата рождения, место рождения, место рождения, адрес проживания и регистрации, семейное положение, образование, профессия, специальность, место работы, занимаемая должность по месту работы, размер получаемых доходов от трудовой деятельности, ИНН, сведения ВУС, СНИЛС, сведения об общем и трудовом стаже, адрес электронной почты, номер телефона, место работы или учебы членов семьи и близких родственников, состав декларируемых сведений о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию, налоговый статус (резидент/нерезидент), иные сведения указанные заявителем.

Персональные данные Работника – информация, необходимая Оператору, как работодателю, в связи с трудовыми отношениями и касающимися конкретного Работника. Под информацией о Работнике понимаются сведения о фактах, событиях и обстоятельствах жизни Работника, позволяющие идентифицировать его личность, в том числе: фамилия, имя, отчество, образование, сведения о составе семьи, сведения о трудовом и общем стаже, паспортные данные, СНИЛС, сведения о воинском учете, ИНН, налоговый статус (резидент/нерезидент), сведения о заработной плате Работника, сведения о социальных льготах, специальность, занимаемая должность, адрес проживания и регистрации, номер телефона, место работы или учебы членов семьи Работника, характер отношений в семье, содержание и условия трудового договора, состав декларируемых сведений о наличии материальных ценностей, содержание декларации, подаваемой в налоговую инспекцию, иную не указанную выше информацию, содержащуюся в личных делах и трудовых книжках, информацию, являющуюся основанием к приказам по личному составу, информацию содержащуюся в страховом медицинском полисе обязательного медицинского страхования граждан, медицинском заключении об отсутствии у гражданина заболевания, препятствующего поступлению на работу в Общество, дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям.

Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Субъект персональных данных – Работник, Клиент, Контрагент.

Защита персональных данных Работника, Клиента, Контрагента – деятельность Общества по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации.

Конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать из распространения без согласия субъекта персональных данных или наличия иного законного основания.

Подразделение ИБ - отдел информационной безопасности и режима Общества, либо работник Общества, на которого возложены обязанности по обеспечению информационной безопасности и режима Общества, в том числе обязанности по организации обработке персональных данных.

Подразделение по работе с персоналом – отдел по работе с персоналом Общества либо работник Общества, на которого возложены обязанности по работе с персоналом.

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

1.3. Персональные данные работников Общества относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 (Семидесяти пяти) лет срока хранения, если иное не определено законодательством Российской Федерации.

1.4. Действия настоящего Положения распространяются на всех Работников, Клиентов и Контрагентов Общества.

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. В целях обеспечения прав и свобод человека и гражданина Общество и (или) его представители при обработке персональных данных должны соблюдать следующие требования:

2.1.1. Обработка персональных данных должна осуществляться на законной и справедливой основе, исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия исполнения договорных обязательств в соответствии с законодательством РФ.

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

2.1.3. Получение Обществом персональных данных может осуществляться как путем представления их самим Работником, Клиентом, Контрагентом так и путем получения их из иных источников.
2.1.4. Персональные данные получаются Обществом непосредственно у самого Работника, Клиента, Контрагента. Если персональные данные Работника возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Общество должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.
2.1.5. Общество не имеет права получать и обрабатывать персональные данные Работника, Клиента, Контрагента о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни Работника, Клиента, Контрагента (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны Обществом только с его письменного согласия.
2.1.6. Общество не имеет право получать и обрабатывать персональные данные Работника, Клиента, Контрагента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.
2.2. К обработке, передаче и хранению персональных данных могут иметь доступ:
- Директор Общества;
- Руководители структурных подразделений по направлению деятельности (доступ к личным данным сотрудников только своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
- сам работник, источник данных;
- другие сотрудники организации при выполнении ими своих служебных обязанностей.
2.3. Использование персональных данных возможно только в соответствии с целями, определившими их получение.
Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено действующим законодательством Российской Федерации.
2.4. При принятии решений, затрагивающих интересы Клиента или Контрагента, Оператор не имеет права основываться на персональных данных Клиента или Контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.
2.5. При идентификации Клиента или Контрагента Общество может затребовать предъявления документов, удостоверяющих личность и подтверждающих полномочия представителя.
2.6. При заключении договора, как и в ходе выполнения договора может возникнуть необходимость в предоставлении Клиентом или Контрагентом иных документов, содержащих информацию о нем.
2.7. После принятия решения о заключении договора или представления документов, подтверждающих полномочия представителя, а так же впоследствии, в процессе выполнения договора, содержащего персональные данные Клиента или Контрагента, к персональным данным также будут относиться:
- договоры;
- приказы по основной деятельности;
- служебные записки;
- приказы о допуске представителя Клиента, Контрагента;
- разовые или временные пропуска;
- другие документы, где включение персональных данных Клиента или Контрагента необходимо согласно действующему законодательству.
2.8. Передача персональных данных возможна только с согласия Работника, Клиента, Контрагента или в случаях, прямо предусмотренных законодательством Российской Федерации.

2.8.1. При передаче персональных данных Общество должно соблюдать следующие требования:
- не сообщать персональные данные третьей стороне без письменного согласия Работника, Клиента, Контрагента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника, Клиента, Контрагента, а также в случаях, установленных законодательством Российской Федерации;
- не сообщать персональные данные в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном законодательством Российской Федерации;
- разрешать доступ к персональным данным только специально уполномоченным лицам, определенным приказом директора Общества, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные Работника представителям Работников в порядке, установленном Трудовым кодексом, и ограничивать эту информацию только теми персональными данными Работника, которые необходимы для выполнения указанными представителями их функций.
2.8.2. Передача персональных данных от Общества и (или) его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
2.8.3. При передаче персональных данных внешним потребителям (в том числе и в коммерческих целях) Общество не должно сообщать эти данные третьей стороне без письменного согласия Работника, Клиента, Контрагента, за исключением случаев, установленных законодательством Российской Федерации.
2.9. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
2.10. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.
2.11. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.
2.12. Период хранения и обработки персональных данных определяется в соответствии с Законом «О персональных данных». Обработка персональных данных начинается с поступления персональных данных в информационные системы персональных данных и прекращается:
- в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления, Общество устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений, Общество в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожает персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Общество уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;
- в случае достижения цели обработки персональных данных Общество незамедлительно прекращает обработку персональных данных и уничтожает соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, и уведомляет об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, Общество уведомляет также указанный орган;
- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Общество прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных Общество уведомляет субъекта персональных данных.

- в случае прекращения деятельности Общества.

2.13. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В поручении оператора должны быть определены: перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2.14. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

2.15. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

3. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

3.1. Список лиц, допущенных к обработке персональных данных (далее - Список) и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение правил обработки персональных данных, определяется и утверждается директором Общества.

3.2. Подразделение по работе с персоналом при принятии на работу, увольнении или изменении должностных обязанностей Работников не позднее чем в трехдневный срок вносит изменения в список лиц, допущенных к обработке персональных данных, по согласованию с Подразделением ИБ.

3.3. Подразделение ИБ, не реже одного раза в квартал, обязано проверять актуальность Списка. В случае выявления расхождений, Подразделение по работе с персоналом вносит изменения в Список.

3.4. Работники Общества выполняют действия по обработке персональных данных в соответствии с возложенными на работников функциями.

3.5. Доступ к персональным данным предоставляется только лицам, замещающим должности из Списка. Предоставление доступа к ИСПДн осуществляется в соответствии с «Инструкцией о порядке допуска лиц к информационным ресурсам ИСПДн и в помещение объекта информатизации ООО «Народный ломбард»».

3.6. Работники имеют доступ на ввод и коррекцию персональных данных в пределах, определенных должностными обязанностями.

3.7. Лица, получившие доступ к персональным данным, должны хранить в тайне известные им сведения конфиденциального характера и информировать Подразделение ИБ об утечке персональных данных, о фактах нарушения порядка обращения с ними, о попытках несанкционированного доступа к персональным данным.

3.8. Лица, получившие доступ к персональным данным, должны использовать эти данные лишь в целях, для которых они сообщены, обязаны соблюдать режим конфиденциальности и дать Обязательство о неразглашении персональных данных.

4. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Все работники, имеющие доступ к персональным данным, обязаны подписать соглашение о неразглашении персональных данных.

4.2. Защита персональных данных от неправомерного их использования или утраты обеспечивается Оператором в порядке, установленном законодательством РФ.

4.3. Работники, клиенты или контрагенты до предоставления своих персональных данных должны иметь возможность ознакомиться с настоящим Положением.

4.4. Защите подлежат:

- информация о персональных данных субъекта;

- документы, содержащие персональные данные субъекта;
- персональные данные, содержащиеся на электронных носителях.

4.5. Оператор назначает ответственного за организацию обработки персональных данных.

4.6. Оператор издает документы, определяющие политику Оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

4.7. Оператор принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в том числе:

1) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учет машинных носителей персональных данных;

6) обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

4.8. Оператор осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требование к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам Оператора.

4.9. Оператор осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом

4.10. Оператор ознакамливает своих работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

4.11. Ответственные лица соответствующих подразделений, хранящих персональные данные на бумажных носителях и машинных носителях информации, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному Постановлением Правительства РФ от 15 сентября 2008 г. № 687.

4.12. Ответственные лица структурных подразделений, обрабатывающие персональные данные в информационных системах персональных данных и машинных носителях информации, обеспечивают защиту в соответствии с Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных» и другими нормативными, нормативно-методическими, методическими документами.
4.13. По возможности персональные данные должны быть обезличены.
4.14. Анализ угроз. Обеспечение безопасности персональных данных, а также разработка и внедрение средств защиты персональных данных основывается на анализе угроз безопасности персональных данных. Общество разрабатывает и поддерживает модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Приложение №1).
Модель угроз отражает актуальное состояние защищенности информационных систем персональных данных и актуальные угрозы безопасности персональных данных. Разработка Частной модели угроз осуществляется на основании анализа существующих угроз безопасности и возможности их реализации в обследуемых информационных системах персональных данных.
4.15. Порядок уничтожения персональных данных. Ответственным за уничтожение персональных данных является уполномоченное лицо, назначаемое приказом директора. Уполномоченное лицо является председателем комиссии Общества по уничтожению персональных данных. Назначение комиссии по уничтожению персональных данных производится приказом директора.
При наступлении любого из событий, повлекших, согласно законодательства РФ, необходимость уничтожения персональных данных, Уполномоченное лицо обязано:
- уведомить членов комиссии о работах по уничтожению персональных данных;
- определить (назначить) время, место работы комиссии (время и место уничтожения персональных данных);
- установить перечень, тип, наименование, регистрационные номера и другие данные носителей, на которых находятся персональные данные подлежащие уничтожению (и/или материальные носители персональных данных);
- определить технологию (прием, способ) уничтожения персональных данных (и/или материальных носителей персональных данных);
- определить технические (материальные, программные и иные) средства, посредством которых будет произведено уничтожение персональных данных;
- руководя работой членов комиссии, произвести уничтожение персональных данных (и/или материальных носителей персональных данных);
- оформить соответствующий Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) и представить Акт об уничтожении персональных данных (и/или материальных носителей персональных данных) на утверждение директору;
- в случае необходимости уведомить об уничтожении персональных данных субъекта персональных данных и/или уполномоченный орган.

5. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА

5.1. Работники и их представители должны быть ознакомлены под расписку с документами Общества, устанавливающими порядок обработки персональных данных Работников, а также об их правах и обязанностях в этой области.
5.2. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:
- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.
5.3. Работник обязан:
- предавать Обществу и/или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации;
- своевременно сообщать Обществу об изменении своих персональных данных.
5.4. Работники ставят Общество в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и прочее.
5.5. В целях защиты частной жизни, личной и семейной тайны работники вправе отказываться от обработки их персональных данных без их согласия.

6. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТОВ И КОНТРАГЕНТОВ

6.1. В целях обеспечения защиты персональных данных, хранящихся у Оператора, Клиент и Контрагенты имеют право на:

6.1.1. Полную информацию о составе персональных данных и их обработке, в частности Клиент или Контрагент имеет право знать, кто и в каких целях использует или использовал информацию о его персональных данных.

6.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные Клиента или Контрагента, за исключением случаев, предусмотренных законодательством РФ.

6.1.3. Определение своих представителей для защиты своих персональных данных.

6.1.4. Требование об исключении или исправлении неверных или неполных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Оператора персональных данных. При отказе Оператора исключить или исправить персональные данные Клиента или Контрагента он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия.

6.1.5. Требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные Клиента или Контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.1.6. Обжалование в суд любых неправомерных действий или бездействия Оператора при обработке и защите его персональных данных.

6.2. В целях обеспечения достоверности персональных данных, Клиент и Контрагент обязаны:

6.2.1. При заключении договора предоставить Оператору полные и достоверные данные о себе;

6.2.2. В случае изменения сведений, составляющих персональные данные Клиента или Контрагента, незамедлительно, но не позднее пяти рабочих дней, предоставить данную информацию Оператору.

7. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

7.1. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.2. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет ответственность за данное разрешение.

7.3. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

7.4.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера Общество вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

7.4.2. Должностные лица, в обязанность которых входит обработка персональных данных, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в представлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.4.3. В соответствии с Гражданским кодексом Российской Федерации лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников Общества.

7.4.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконный сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном

порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом.

7.5. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

8. ОБЯЗАННОСТИ РАБОТНИКОВ ПО ОХРАНЕ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ

8.1. В целях охраны конфиденциальности информации все работники обязаны:

8.1.1. Не разглашать сведения, составляющие коммерческую тайну Общества, за исключением случаев, когда есть письменное согласие руководителя Общества.

8.1.2. Не использовать сведения, составляющие коммерческую тайну Общества, для занятия другой деятельностью, в процессе работы для другой организации, предприятия, учреждения, по заданию физического лица или в ходе осуществления предпринимательской деятельности, а также в личных целях.

8.1.3. Выполнять установленный Обществом режим коммерческой тайны.

8.1.4. Незамедлительно ставить в известность непосредственного руководителя и руководителя Общества о необходимости отвечать либо об ответах на вопросы должностных лиц компетентных органов (налоговая инспекция, органы предварительного следствия и т.п.), находящихся при исполнении служебных обязанностей, по вопросам коммерческой тайны Общества.

8.1.5. Незамедлительно сообщать непосредственному руководителю и руководителю Общества об утрате или недостаче носителей информации, составляющих коммерческую тайну, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению коммерческой тайны Общества, а также о причинах и условиях возможной утечки информации, составляющей коммерческую тайну Общества.

8.1.6. В случае попытки посторонних лиц получить от работника сведения, содержащие коммерческую тайну Общества, незамедлительно известить об этом непосредственного руководителя и руководителя Общества.

8.1.7. Не создавать условий для утечки информации, составляющей коммерческую тайну Общества, и предпринимать все усилия для пресечения такой утечки, если ему стало известно, что утечка имеет место или что складываются условия для возможности таковой.

8.1.8. Не разглашать и не использовать для себя или других лиц сведения, составляющие коммерческую тайну Общества, в течение трех лет после прекращения трудового договора с Обществом (независимо от причин увольнения).

8.1.9. Передать Обществу при прекращении трудового договора или гражданско-правового договора имеющиеся в пользовании Работника материальные носители с информацией, составляющей коммерческую тайну.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Настоящее Положение вступает в силу с момента его утверждения.

9.2. Настоящее Положение доводится до сведения всех работников Общества персонально под роспись.

Приложение №1
к Положению о защите
персональных данных
работников, клиентов
и контрагентов

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторизация - предоставление прав доступа.

Актив - все, что имеет ценность для Общества и находится в распоряжении Общества.

Архитектура объектов информатизации - совокупность основных структурно-функциональных характеристик и свойств объектов информационной инфраструктуры, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

Безопасность - состояние защищенности интересов (целей) Общества в условиях угроз.

Документация - совокупность взаимосвязанных документов, объединенных общей целевой направленностью.

Допустимый риск нарушения информационной безопасности - риск нарушения информационной безопасности, предполагаемый ущерб от которого Общества в данное время и в данной ситуации готова принять.

Доступность информационных активов - свойство информационной безопасности Общества, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

Защитная мера - сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения информационной безопасности Общества.

Идентификация - процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность - безопасность, связанная с угрозами в информационной сфере.

Информационная инфраструктура - система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия.

Информационный актив - информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для Общества, находящаяся в распоряжении Общества и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Инцидент информационной безопасности - событие или комбинация событий, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы безопасности информации, результатом которой являются:

• нарушение или возможное нарушение работы средств защиты информации в составе системы обеспечения информационной безопасности Общества;

• нарушение или возможное нарушение требований законодательства Российской Федерации, нормативных актов и предписаний регулирующих и надзорных органов, внутренних документов Общества в области обеспечения информационной безопасности, нарушение или

возможное нарушение в выполнении процессов системы обеспечения информационной безопасности Общества;

• нарушение или возможное нарушение в выполнении технологических процессов Общества;

• нанесение или возможное нанесение ущерба Обществу и (или) его клиентам.

Конфиденциальность информационных активов - свойство информационной безопасности Общества, состоящее в том, что обработка, хранение и передача информационных активов осуществляются таким образом, что информационные активы доступны только авторизованным пользователям, объектам системы или процессам.

Информационная система - система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают и распространяют информацию.

Модель нарушителя информационной безопасности - описание и классификация нарушителей информационной безопасности, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз информационной безопасности со стороны указанных нарушителей.

Модель угроз информационной безопасности - описание актуальных для Общества источников угроз безопасности информации; методов реализации угроз безопасности информации; объектов, пригодных для реализации угроз безопасности информации; уязвимостей, используемых источниками угроз безопасности информации; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.

Мониторинг - постоянное наблюдение за объектами и субъектами, влияющими на информационную безопасность Общества, а также сбор, анализ и обобщение результатов наблюдений.

Нарушитель информационной безопасности - субъект, реализующий угрозы безопасности информации Общества, нарушая предоставленные ему полномочия по доступу к активам Общества или по распоряжению ими.

Обработка риска нарушения информационной безопасности - процесс выбора и осуществления защитных мер, снижающих риск нарушения информационной безопасности, или мер по переносу, принятию или уходу от риска.

Риск нарушения информационной безопасности - риск, связанный с угрозой безопасности информации.

Система информационной безопасности - совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Угроза информационной безопасности - угроза нарушения свойств информационной безопасности – доступности, целостности или конфиденциальности информационных активов Общества.

1. Настоящий внутренний документ является методикой моделирования угроз безопасности информации и разработан с учетом условий и особенностей функционирования информационных систем Общества, с учетом требований законодательства Российской Федерации в области обеспечения информационной безопасности.

2. Целью моделирования угроз безопасности информации является выявление совокупности условий и факторов, которые приводят или могут привести к нарушению безопасности обрабатываемой информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств её обработки), а также к нарушению или прекращению функционирования объектов информационной инфраструктуры.

3. В качестве угроз безопасности информации, подлежащих определению при моделировании угроз безопасности информации, рассматриваются неправомерные действия и (или) воздействия на объекты информационной инфраструктуры, в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования систем и сетей, повлекшее наступление негативных последствий.

4. В результате моделирования угроз безопасности информации формируется перечень актуальных угроз безопасности информации, реализуемых в информационной инфраструктуре Общества.

5. Процесс моделирования угроз безопасности информации включает:

– определение возможных негативных последствий от реализации угроз безопасности информации;

– определение условий для реализации угроз безопасности информации;

– определение источников угроз безопасности информации и оценку возможностей нарушителей;

– определение сценариев реализации угроз безопасности информации;

– оценку уровня опасности угроз безопасности информации.

Процесс моделирования угроз безопасности информации

Входные данные	**Этап**	**Получаемый результат**
Требования законодательства Российской Федерации	Определение возможных негативных последствий от реализации угроз безопасности информации	Перечень возможных негативных последствий
Сведения о структурно-функциональных характеристиках информационной инфраструктуры		Информационные активы
Результаты оценки рисков		Виды неправомерного доступа и (или) воздействий
Сведения об информационных активах		Перечень угроз безопасности информации
Сведения о структурно-функциональных характеристиках информационной инфраструктуры	Определение условий для реализации угроз безопасности информации	Типы уязвимостей и (или) недекларированных возможностях
Сведения об уязвимостях		Варианты возможного доступа нарушителей информационной безопасности к объектам информационной инфраструктуры
Сведения о доступе к объектам информационной инфраструктуры		
Особенности организации технологических процессов Общества	Определение источников угроз безопасности информации и оценку возможностей нарушителей	Виды источников угроз безопасности информации
Сведения о сервисах, предоставляемых сторонними организациями		Возможные цели реализации угроз безопасности информации нарушителями
Сведения о типах внутренних и внешних пользователей		Категории, виды и возможности нарушителей
Сведения об объектах информационной инфраструктуры и особенностях их функционирования	Определение сценариев реализации угроз безопасности информации	Перечень сценариев угроз безопасности информации
Условия реализации угроз безопасности информации		
Категории, виды и возможности нарушителей		
Перечень сценариев реализации угроз безопасности информации	Оценка уровня опасности угроз безопасности информации	Уровни опасности угроз безопасности информации
Сведения о типе доступа к		

объектам информационной инфраструктуры		
Сведения о сложности реализации сценария		
Сведения об уровне значимости объектов информационной инфраструктуры		

6. При моделировании угроз безопасности информации определяется граница процесса моделирования, в которую включаются объекты информационной инфраструктуры, обрабатывающие, хранящие информацию и (или) обеспечивающие реализацию основных бизнес-процессов, интерфейсы их взаимодействия с пользователями, со смежными (взаимодействующими) объектами информационной инфраструктуры, а также инженерные системы (системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны, системы охраны), средства, каналы и услуги связи, другие услуги и сервисы, предоставляемые сторонними организациями, от которых зависит функционирование объектов информационной инфраструктуры.

7. Информационные активы Общества рассматриваются в совокупности с соответствующими им объектами среды. При этом обеспечение информационной безопасности для информационных активов выражается в создании необходимой защиты соответствующих им объектов среды.

8. Формирование перечней типов объектов среды выполняется в соответствии с иерархией уровней информационной инфраструктуры Общества.

9. На каждом из уровней информационной инфраструктуры угрозы и их источники, методы и средства защиты и подходы к оценке эффективности являются различными:

Уровни информационной инфраструктуры	**Объекты среды**	**Способы реализации угроз**
Физический уровень	Физические носители информации, в составе системы хранения данных Физические носители информации, в составе системы резервного копирования Физические носители информации, в составе автоматизированных рабочих мест Съемные носители информации Каналы связи Мониторы Помещения/здания/сооружения Технические средства информационных систем	Хищение/кража Утрата Уничтожение/разрушение Несанкционированный физический доступ Утечка информации
Сетевой уровень	Коммуникационное оборудование	Атаки типа «отказ в обслуживании» Нарушение штатных режимов работы сетевого оборудования Внедрение аппаратных закладок

Уровень сетевых приложений и сервисов	Сетевые приложения и сервисы	Внедрение вредоносного программного обеспечения Анализ трафика Атаки типа «отказ в обслуживании» Использование специализированных программ Нарушение штатных режимов работы сетевых приложений Отказ от авторства Сканирование сети, направленное на выявление открытых портов и служб, открытых соединений
Уровень операционных систем	Файлы данных с информацией ограниченного распространения Общесистемные программные средства Информация, необходимая для идентификации, аутентификации и (или) авторизации Файлы данных с открытой информацией	Кража (утеря, компрометация) пароля Копирование Модификация/удаление Нарушение штатных режимов работы ОС Распространение вредоносных программ Неправильное (не полное) конфигурирование СЗИ Несанкционированный доступ в ОС с использованием специализированного ПО
Уровень систем управления базами данных	Базы данных информационных систем Информация, необходимая для идентификации, аутентификации и (или) авторизации	Копирование Неправильное (не полное) конфигурирование СЗИ Модификация/удаление Нарушение штатных режимов работы СУБД Подмена пользовательских идентификаторов Несанкционированный логический доступ к СУБД Распространение вредоносных программ Кража пароля
Уровень технологических процессов и приложений	Программное обеспечение, предназначенное для обработки защищаемой информации Программное обеспечение, предназначенное для обработки открытой информации Информация, необходимая для идентификации, аутентификации и (или) авторизации Ключевые носители Бумажные документы	Отказ от авторства Модификация/удаление Распространение/передача Печать документов Нарушение штатных режимов работы приложений Кража документов Кража пароля
Уровень бизнес-процессов	Информационные активы (сведения ограниченного доступа) люди	Непреднамеренное нарушение бизнес-процесса Преднамеренное нарушение бизнес-процесса

9.1. В зависимости от архитектуры и условий функционирования объектов информационной инфраструктуры для реализации угроз безопасности информации может быть использован удаленный, локальный или физический доступ к объектам информационной инфраструктуры.

9.2. Удаленный доступ при реализации угроз безопасности информации осуществляется нарушителем из-за границ контролируемой зоны при его взаимодействии с сетями связи общего пользования, в первую очередь с сетью Интернет. При удаленном доступе воздействия на объекты информационной инфраструктуры реализуются посредством сетевых протоколов.

9.3. Локальный доступ при реализации угроз безопасности информации может осуществляться нарушителем в пределах границ контролируемой зоны. При локальном доступе неправомерный доступ и (или) воздействие на объекты информационной инфраструктуры реализуются при наличии и использовании локальной учетной записи пользователя, зарегистрированной в системе. Удаленное использование нарушителем локальной учетной записи пользователя, в том числе из взаимодействующей (смежной) системы или сети Интернет, при реализации угрозы безопасности информации относится к локальному доступу.

9.4. Физический доступ для реализации угроз безопасности информации может осуществляться нарушителями в пределах границ контролируемой зоны и при наличии у них непосредственного физического доступа к объектам информационной инфраструктуры. Целью физического доступа нарушителя также может являться получение локального доступа для реализации локальных угроз безопасности информации. В этом случае оценке подлежат угрозы безопасности информации, связанные с локальным доступом к объектам информационной инфраструктуры.

9.5. Для непреднамеренных угроз безопасности информации условием их возникновения является наличие у внутреннего нарушителя локального и (или) физического доступа к системам и сетям. При этом внутренний нарушитель может иметь привилегированные или непривилегированные права по доступу к объектам информационной инфраструктуры.

10. При моделировании угроз безопасности информации оценке подлежат угрозы безопасности информации, связанные со всеми типами источников. В целях создания и эксплуатации адекватной эффективной системы защиты необходимо уделять внимание оценке антропогенных источников угроз, связанных с действиями нарушителей. Оценка возможностей нарушителей включает определение категорий, видов нарушителей, их компетенции и оснащенности, которыми они могут обладать для реализации угроз безопасности информации.

10.1. Модель нарушителя содержит описание предположений о возможностях нарушителя (злоумышленника), которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

10.2. Нарушитель может действовать на различных этапах жизненного цикла информационных систем, обрабатывающих информационные активы Общества.

10.3. Главной целью нарушителя является получение контроля над информационными активами на уровне бизнес-процессов. Прямое нападение на уровне бизнес-процессов более эффективно для нарушителя и опаснее для собственника, чем нападение, осуществляемое через нижние уровни, но при этом более сложное для реализации, в связи с чем, атаки злоумышленника на объекты среды уровня бизнес-процессов рассматриваются как совокупность атак на более низкие уровни информационной инфраструктуры.

10.4. Все физические лица, имеющие доступ к техническим и программным средствам, разделяются на следующие категории: − категория I – лица, не имеющие права доступа в помещения, где расположены технические и программные средства; − категория II – лица, имеющие право постоянного или разового доступа в помещения, где расположены технические и программные средства.

10.5. Все потенциальные нарушители подразделяются на: − внешних нарушителей, осуществляющих атаки вне пределов контролируемой зоны Общества; − внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны Общества.

10.6. Таким образом, внешними нарушителями могут быть как лица категории I, так и лица категории II, а внутренними нарушителями могут быть только лица категории II.

10.7. Основные источники угроз безопасности информации:

Типы источников угроз безопасности информации	**Источники угроз безопасности информации**
Компьютерные	Хакер

злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе использование компьютерных вирусов и других типов вредоносных	Компьютерный хулиган
Сотрудники Общества, являющиеся легальными участниками процессов в информационных системах и действующие в рамках предоставленных полномочий	Пользователи информационных систем
	Администраторы информационных систем и средств защиты информации
	Технический персонал, имеющий доступ к аппаратному обеспечению
Сотрудники Общества, являющиеся легальными участниками процессов в информационных системах и действующие вне рамок предоставленных полномочий	Администраторы информационных систем и средств защиты информации
	Пользователи информационных систем
	Технический персонал, имеющий доступ к аппаратному обеспечению
Неблагоприятные события природного и техногенного характера	Пожары
	Наводнения, землетрясения, извержения вулканов, ураганы, смерчи, тайфуны, цунами и т.д.
	Техногенные катастрофы
	Нарушение внутриклиматических условий
	Нарушение или снижение качества электропитания
	Сбои и аварии в системах водоснабжения, канализации, отопления
Террористы, криминальные элементы	Террористы
	Криминальные элементы
	Недобросовестные конкуренты
Провайдеры	Провайдер канала связи
	Интернет-провайдер
Подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования и его ремонт	Сотрудник технической поддержки
	Сервисный инженер
	Разработчик программного обеспечения
	Разработчик технических средств
Внешние нарушители, имеющие доступ к ИС	Аудитор
	Партнер
	Клиент
	Сотрудник Надзорного ведомства

11. Моделирование угроз безопасности информации носит систематический характер и осуществляться как на этапе создания объектов информационной инфраструктуры и формирования требований по их защите, так и в ходе их эксплуатации. Систематический подход к моделированию угроз безопасности информации позволяет поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных активов. Учет изменений угроз безопасности информации способствует своевременной выработке адекватных мер защиты информации.

12. На этапе создания объектов информационной инфраструктуры моделирование угроз безопасности информации проводится на основе их предполагаемой архитектуры и направлено на обоснованный выбор организационных мер, функциональных возможностей и настроек средств защиты информации. На этапе эксплуатации – моделирование угроз безопасности информации проводится для реальной архитектуры объектов информационной инфраструктуры и условий их функционирования и направлено на выявление изменений угроз безопасности информации и оценку эффективности применяемых мер и средств защиты информации.

13. Моделирование угроз безопасности информации проводится с учетом применяемых на объектах информационной инфраструктуры в соответствии с требованиями нормативных правовых актов Российской Федерации и (или) технических заданий средств защиты информации. Однако при этом учитывается возможность наличия в организации работ и применяемых средствах защиты информации уязвимостей, которые могут использоваться для реализации угроз безопасности информации.

14. Моделирование угроз безопасности информации проводится отделом автоматизации и информационного сопровождения. К моделированию угроз безопасности информации могут привлекаться организации, имеющие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

15. Результаты моделирования угроз безопасности информации отражаются в модели угроз, которая представляет собой формализованное описание актуальных угроз безопасности информации.

16. Модель угроз безопасности информации формируется применительно ко всем объектам информационной инфраструктуры, которые были включены в границу процесса моделирования угроз безопасности информации. По решению Руководства Общества модель угроз безопасности информации может разрабатываться для отдельной системы или сети.

17. Модель угроз безопасности информации должна поддерживаться в актуальном состоянии в процессе функционирования объектов информационной инфраструктуры.

18. Модель угроз применяется при решении следующих задач:

– анализа защищенности от угроз безопасности информационных активов Общества в ходе организации и выполнения работ по обеспечению безопасности информации;

– разработки системы защиты информации, обеспечивающей нейтрализацию угроз с использованием методов и способов защиты информации; – проведения мероприятий, направленных на предотвращение несанкционированного доступа в информационные системы и к обрабатываемым в них информационным активам, включая предотвращение несанкционированного воздействия на технические и программные средства информационных систем;

– контроля за обеспечением уровня защищенности информационных активов;

– определения совокупности условий и факторов, создающих опасность нарушения характеристик безопасности;

– определения типов источников угроз.

19. Изменение модели угроз безопасности информации осуществляется в случаях:

– изменения требований нормативных правовых актов Российской Федерации и методических документов ФСТЭК России, в том числе нормативных актов Банка России, регламентирующих вопросы моделирования угроз безопасности информации;

– изменения архитектуры и условий функционирования объектов информационной инфраструктуры, порядка обработки информации, влияющих на угрозы безопасности информации;

– выявления, в том числе по результатам внешнего или внутреннего контроля эффективности защиты информации (аудита, тестирований на проникновение), новых угроз безопасности информации или новых сценариев реализации существующих угроз.

– выявление уязвимостей, приводящих к возникновению новых угроз безопасности информации или к повышению возможности реализации существующих;

– появления сведений и фактов о новых возможностях нарушителей.

20. При проведении внутреннего или внешнего контроля эффективности защиты информации (аудита, тестирований на проникновение) перед организациями, проводящими такие работы, должна ставиться задача по выявлению максимально возможного числа сценариев реализации существующих угроз безопасности информации, а также задача выявления новых угроз безопасности информации, приводящих к наступлению негативных последствий.