УТВЕРЖДАЮ
ИП Чернов Глеб Анатольевич

_____/ Чернов Г.А.
«27» мая 2025 г.

Политика ИП Чернов Глеб Анатольевич
об обеспечении безопасности персональных данных

1. Меры по обеспечению безопасности персональных данных при их обработке.

1.1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать 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.

1.2. Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– применением 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;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением 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;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

1.3. Для целей Положения под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационной системе персональных данных.

2. Защищаемые сведения о субъекте персональных данных и объекты персональных данных.

2.1. К защищаемым сведениям о субъекте персональных данных относятся данные, позволяющие идентифицировать субъект персональных данных и/или получить о нем дополнительные сведения, предусмотренные законодательством и Политикой.

2.2. Защищаемые объекты персональных данных.

2.2.1. К защищаемым объектам персональных данных относятся:

– объекты информатизации и технические средства автоматизированной обработки информации, содержащей персональные данные;

– информационные ресурсы (базы данных, файлы и др.), содержащие информацию об информационно-телекоммуникационных системах, в которых циркулируют персональные данные, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

– каналы связи, которые используются для передачи персональных данных в виде информативных электрических сигналов и физических полей;

– отчуждаемые носители информации на магнитной, магнитно-оптической и иной основе, применяемые для обработки персональных данных.

2.2.2. Технологическая информация об информационных системах и элементах системы защиты персональных данных, подлежащая защите, включает:

– сведения о системе управления доступом на объекты информатизации, на которых осуществляется обработка персональных данных;

– 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.);

– характеристики каналов связи, которые используются для передачи персональных данных в виде информативных электрических сигналов и физических полей;

– информация о средствах защиты персональных данных, их составе и структуре, принципах и технических решениях защиты;

– служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки персональных данных.

3. Требования к системе защиты персональных данных.

3.1. Система защиты персональных данных должна соответствовать требованиям постановления Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.2. Система защиты персональных данных должна обеспечивать:

– своевременное обнаружение и предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

– недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– постоянный контроль за обеспечением уровня защищенности персональных данных.

3.3. Средства защиты информации, применяемые в информационных системах, должны в установленном порядке проходить процедуру оценки соответствия.

4. Методы и способы защиты информации в информационных системах персональных данных.

4.1. Методы и способы защиты информации в информационных системах персональных данных Оператора должны соответствовать требованиям:

– приказа ФСТЭК 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 ФСБ от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (в случае определения Оператором необходимости использования средств криптографической защиты информации для обеспечения безопасности персональных данных).

4.2. Основными методами и способами защиты информации в информационных системах персональных данных являются методы и способы защиты информации от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий (далее – методы и способы защиты информации от НСД).

4.3. Выбор и реализация методов и способов защиты информации осуществляется в соответствии с рекомендациями регуляторов в области защиты информации – ФСТЭК России и ФСБ России, с учетом определяемых Оператором угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы.

4.4. Выбранные и реализованные методы и способы защиты информации должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке.

5. Меры защиты информации, составляющей персональные данные.

5.1. Меры по охране баз данных, содержащих персональные данные, принимаемые Оператором, должны включать в себя:

– определение перечня информации, составляющей персональные данные;

– ограничение доступа к информации, содержащей персональные данные, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

5.2. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

– исключается доступ к персональным данным любых третьих лиц без согласия Оператора;

– обеспечивается возможность использования информации, содержащей персональные данные, без нарушения законодательства о персональных данных;

– при работе с Субъектом устанавливается такой порядок действий Оператора, при котором обеспечивается сохранность сведений, содержащих персональные данные Субъекта.

5.3. Оператор применяет, в частности, следующие правовые, организационные и технические меры по обеспечению безопасности персональных данных:

Выбрать нужное либо внести иное:

- установлением индивидуальных паролей доступа работников Оператора в информационную систему в соответствии с их производственными обязанностями.
- сертифицированным антивирусным программным обеспечением с регулярно обновляемыми базами.
- использованием SSL – протоколов, антивирусного программного обеспечения, межсетевых экранов;
- использованием лицензионных программных продуктов, предотвращающих несанкционированный доступ третьих лиц к персональным данным;
- использованием системы паролей условно-постоянного действия длинной не менее шести буквенно-цифровых символов. Пароли устанавливаются системным администратором и сообщаются индивидуально работникам, имеющим доступ к персональным данным пользователей, работников, кандидатов для приема на работу и бывших работников;
- наличием средств восстановления системы защиты персональных данных;
- использованием средств резервного копирования;
- передачей данных по защищенным каналам связи;
- ведением учета машинных носителей информации;
- выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением физической охраны/вневедомственной охраны/сигнализации, в целях контроля доступа посторонних лиц в офисные помещения Оператора;
- работники Оператора, допущенные к работе с персональными данными обязаны соблюдать меры по обеспечению безопасности персональных данных в том числе:

• не передавать свой пароль от входа в информационную систему третьим лицам;

• по окончании работы в системе – завершить сеанс пользователя;

• не допускать хранения в открытом доступе документов, содержащих конфиденциальную информацию;

5.6. Персональные данные не могут быть использованы в целях, противоречащих требованиям Федерального закона, защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

6. Ответственность.

6.1. Все работники Оператора, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с Положением, требованиями законодательства РФ.

6.2. Лица, виновные в нарушении требований Политики, несут предусмотренную законодательством РФ ответственность.

6.3. Ответственность за соблюдение режима персональных данных по отношению к персональным данным, находящимся в базах данных, несут ответственные за обработку персональных данных.