СВЕДЕНИЯ
о реализуемых требованиях к защите персональных данных
в управлении лесами Правительства Хабаровского края

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" в управлении лесами Правительства Хабаровского края (далее – Управление) внедрены правовые, организационные и технические меры для защиты обрабатываемых персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

Управлением реализованы следующие требования к защите персональных данных:

1. Управление включено в реестр операторов персональных данных 26.01.2011 под регистрационным номером 11-0171804.

2. Назначен ответственный за организацию обработки персональных данных (один из заместителей начальника управления), определены его должностные обязанности.

3. Утверждены приказами Управления:

перечень персональных данных;

политика в отношении обработки персональных данных;

правила обработки персональных данных;

правила рассмотрения запросов субъектов персональных данных (их представителей);

правила осуществления внутреннего контроля;

перечень информационных систем персональных данных;

перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

должностные обязанности лица, ответственного за организацию обработки персональных данных;

типовые формы согласия на обработку персональных данных:

- гражданского служащего (работника);
- гражданина, изъявившего желание участвовать в конкурсе на замещение вакантной должности гражданской службы края и (или) на включение в кадровый резерв;
- лица, изъявившего желание участвовать в конкурсе на замещение вакантной должности руководителя краевого государственного учреждения, подведомственного Управлению и (или) на включение в кадровый резерв;
- руководителя краевого государственного учреждения, подведомственного Управлению;
- субъекта персональных данных;

типовое обязательство гражданского служащего (работника) в случае расторжения с ним служебного контракта или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных (трудовых) обязанностей;

типовые формы разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в связи с поступлением на гражданскую службу и её прохождением (поступлением на работу и её выполнением);

порядок доступа в помещения Управления, в которых ведется обработка персональных данных.

4. Персональные данные защищены от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

5. Выполнены требования, установленные для обработки персональных данных без использования средств автоматизации.

6. Организован режим обеспечения безопасности помещений, в которых ведется обработка персональных данных с использованием информационной системы либо без использования средств автоматизации, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, в том числе:

– организован пропускной режим в здание управления;

– служебные помещения оборудованы дверями с замками;

– определен перечень лиц, осуществляющих обработку персональных данных либо имеющих доступ к персональным данным;

– определен перечень лиц, имеющих доступ к персональным данным, в связи с выполнением ими обязанностей по обслуживанию технических средств информационных систем персональных данных;

– допуск посетителей в служебные помещения осуществляется только в присутствии служащих (работников) управления;

– служебные помещения оборудованы средствами охранной и пожарной сигнализации;

– ведется круглосуточное видеонаблюдение за периметром и коридорами здания управления.

7. Хранение персональных данных организовано: на машинных носителях – с использованием средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации; на бумажных носителях – в сейфах (шкафах), исключающих несанкционированный доступ.

8. Приняты правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с установленным уровнем защищенности, в том числе:

8.1.Назначены ответственные должностные лица: за администрирование системы защиты информации, в том числе обеспечение безопасности персональных данных, в информационной системе; за управление идентификаторами и средствами аутентификации в информационной системе; за обращение со средствами криптографической защиты информации.

8.2.Определена информационная система персональных данных в Управлении.

8.3.Разработана модель угроз безопасности в информационной системе (на основании "Базовой модели угроз безопасности в информационных системах Правительства Хабаровского края").

8.4.Определен требуемый уровень защищенности персональных данных при их обработке в информационной системе (третий уровень защищенности).

8.5.Место нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации, — Российская Федерация, Хабаровский край, г. Хабаровск, ул. Запарина, д. 5.

8.6.Все машинные носители информации поставлены на учет, обеспечен запрет использования незарегистрированных съемных носителей информации.

8.7.Реализована система резервирования информации.

8.8.Введена разрешительная система доступа субъектов доступа к объектам доступа в информационной системе.

8.9.Определены перечень регистрируемых событий безопасности в информационной системе, правила и процедуры регистрации событий безопасности, обеспечена регистрация действий, совершаемых с персональными данными.

8.10. Средства обеспечения безопасности в информационной системе:

все рабочие станции и серверы, функционирующие в среде виртуализации, защищены сертифицированными средствами аутентификации и идентификации, антивирусной защиты, защиты информации от несанкционированного доступа, серверы – средствами защиты среды виртуализации;

обновление операционных систем осуществляется из Центра сертифицированных обновлений;

обновление антивирусных баз осуществляется ежедневно в автоматическом режиме с официальных сайтов производителей;

проверка уязвимостей, анализ защищенности информационной системы обеспечиваются сертифицированным сетевым сканером безопасности;

применяемое для защиты информации в информационной системе сертифицированное программное обеспечение, включая пакеты сертификации операционных систем, является разработкой российских производителей;

доступ к информационно-телекоммуникационной сети Интернет и внешним информационным ресурсам обеспечивается через корпоративную сеть передачи данных Правительства Хабаровского края, подключение осуществляется через сертифицированное средство криптографической защиты.

8.11. Проведена оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы.

8.12. Информационная система аттестована по требованиям безопасности информации и соответствует третьему уровню защищенности персональных данных, аттестат соответствия требованиям по безопасности информации выдан АО НТЦ "ЭКВИТ", действителен до 31.10.2021.

9. Осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационной системы.

10. Осуществляется внутренний контроль, проводятся периодические проверки условий обработки персональных данных.

11. Гражданские служащие (работники) ознакомлены 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, и локальными актами по вопросам обработки персональных данных.

12. Документ, определяющий политику Управления в отношении обработки персональных данных, опубликован на официальном сайте Управления.