

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных при их обработке в информационных системах

1. Общие положения

1.1. Положение регулирует организацию защиты персональных данных при их обработке в информационных системах Общества, включая учетные записи работников, средства хранения документов, официальный сайт и образовательную платформу «Антитренинги».

1.2. В работе применяются требования статьи 19 Федерального закона № 152-ФЗ, постановления Правительства Российской Федерации от 01.11.2012 № 1119 и действующих нормативных правовых актов уполномоченных органов в сфере технической защиты информации.

1.3. Конкретный состав мер защиты каждой информационной системы устанавливается после определения обрабатываемых данных, модели актуальных угроз и требуемого уровня защищенности. Настоящее Положение определяет обязательные организационные правила и не заменяет документы, составляемые по итогам указанной оценки.

2. Организация безопасности и учет систем

2.1. Директор организует защиту информации, определяет ответственных за ведение информационных систем и утверждает перечень лиц с доступом к персональным данным. При отсутствии выделенного технического специалиста функции контроля возлагаются на директора; технические работы могут выполняться привлеченным специалистом на основании договора.

2.2. В Обществе ведется перечень информационных систем, в которых обрабатываются персональные данные, с указанием их назначения, вида обрабатываемых данных, владельца либо поставщика программного средства, ответственного пользователя, мест хранения и способов доступа.

2.3. Для используемых внешних сервисов проверяются условия договора, наличие обязательств по конфиденциальности и безопасности, порядок

реагирования на инциденты, сроки хранения и возврата либо удаления данных после прекращения сотрудничества.

2.4. Обработка данных в составе образовательной платформы «Антитренинги» организуется таким образом, чтобы администратор, преподаватель и обучающийся получали доступ только к необходимым им разделам и сведениям.

3. Доступ к информационным системам

3.1. Доступ к служебным ресурсам предоставляется по решению директора на основании служебной необходимости. Для каждой учетной записи устанавливается перечень разрешенных операций.

3.2. Пароли учетных записей не подлежат передаче третьим лицам, указанию в заявлениях и открытой переписке. При подозрении на компрометацию пароль незамедлительно заменяется, а предоставленный доступ пересматривается.

3.3. При наличии технической возможности используются многофакторная аутентификация, блокировка рабочего сеанса и разграничение прав доступа. Права администратора предоставляются лишь лицам, которым они необходимы для исполнения функций.

3.4. При увольнении работника либо прекращении действия договора доступ прекращается, служебные носители и ключи доступа возвращаются, а неиспользуемые учетные записи блокируются либо удаляются с соблюдением требований по хранению учетных записей и журналов событий.

4. Меры защиты рабочих мест и электронных документов

4.1. Рабочие места, используемые для обработки персональных данных, должны иметь средства ограничения доступа пользователей, актуальные обновления программного обеспечения, антивирусную защиту, если она применима к используемой системе, и средства предотвращения несанкционированного доступа.

4.2. На рабочем месте запрещается оставлять открытыми доступные посторонним лицам сведения о работниках и обучающихся. При временном отсутствии пользователь блокирует сеанс и обеспечивает сохранность бумажных носителей.

4.3. Передача файлов, содержащих персональные данные, по электронной почте или через сервис обмена сообщениями допускается только в связи с законной целью обработки, с проверкой адресата и соблюдением установленных требований безопасности. Общедоступные ссылки на такие файлы не создаются.

4.4. Резервное копирование, проверка восстановления данных, учет событий безопасности и обновление программных средств проводятся с периодичностью и в объеме, установленными для конкретной информационной системы. Параметры документируются уполномоченным лицом.

4.5. Не допускается использование личных аккаунтов и общедоступных внешних сервисов для хранения персональных данных Общества без правового основания, документально оформленного решения и проверки мер защиты.

5. Реагирование на инциденты

5.1. Инцидентом считается событие, которое привело либо может привести к неправомерному раскрытию, утрате, изменению, блокированию или уничтожению персональных данных: ошибочная отправка, публикация файла, утрата носителя, неправомерный доступ к учетной записи и иные аналогичные обстоятельства.

5.2. Обнаруживший инцидент работник немедленно сообщает директору или ответственному за организацию обработки данных, не удаляет следы инцидента и выполняет полученные указания по прекращению неправомерной обработки.

5.3. Ответственное лицо фиксирует дату и время выявления, информационные системы, предположительно затронутые категории данных, принятые меры, ведет внутреннее расследование и готовит предусмотренные законодательством уведомления.

5.4. Если инцидент соответствует условиям части 3.1 статьи 21 Федерального закона № 152-ФЗ, Общество уведомляет Роскомнадзор в течение 24 часов о выявлении и в течение 72 часов сообщает результаты внутреннего расследования с учетом требований закона.

5.5. По итогам расследования директор принимает меры по устранению причин инцидента, ограничению последствий, корректировке прав доступа и локальных правил.

6. Контроль и пересмотр мер безопасности

6.1. Не реже одного раза в год ответственное лицо оценивает актуальность перечня систем, состав обрабатываемых данных, полномочия пользователей, состояние средств защиты и соблюдение условий договоров с сервисами.

6.2. При внедрении новой образовательной платформы, изменении инфраструктуры или обрабатываемых категорий данных проводится повторная проверка угроз и достаточности принятых мер. Результаты оформляются внутренним документом.

6.3. Содержание настоящего Положения доводится до работников, имеющих доступ к информационным системам персональных данных, под подпись; нарушения рассматриваются в порядке законодательства и применимых договоров.

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ, ОБРАБАТЫВАЮЩИХ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

№	Система / сервис	Цель обработки и категории данных	Ответственное лицо / владелец	Основание использования, меры защиты
1	Образовательная платформа «Антитренинги»	Доступ к курсу, обучение, задания и результаты	Директор / уполномоченный работник	Условия договора с ООО «Интернет университет»; меры по договору и настройкам доступа
2	Официальный сайт Общества	Заявки, обращения и технические данные при наличии соответствующих форм	Директор / уполномоченный работник	Договор на домен/размещение; фактически используемые сервисы
3	Рабочие компьютеры и учетные системы	Кадровые, договорные и учебные сведения в соответствующих целях	Директор / уполномоченный работник	Право на оборудование и ПО; индивидуальные права доступа