|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | Утверждаю | | |
|  | | Директор ООО «» | | |
|  |  | |  | \_\_\_\_\_\_\_ |
|  | | «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. | | |

Регламент

проведения мероприятий по контролю обработки и защиты персональных данных

1. **Внутренний контроль**

Контроль за состоянием защиты информации (далее — контроль) в информационной системе персональных данных ООО «» осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию, а также хищения персональных данных.

Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты информации, решений Федеральной службы по техническому и экспортному контролю (ФСТЭК России), а также в оценке обоснованности и эффективности, принятых мер защиты для обеспечения выполнения утвержденных требований и норм по защите информации.

Постоянный контроль за состоянием защиты информации в ООО «» осуществляется сотрудником, ответственным за обеспечение безопасности персональных данных. Постоянный контроль осуществляется на основании ежегодно утверждаемого директором ООО «» «Плана проведения внутренних контрольных мероприятий (проверок соблюдения требований по защите персональных данных) в ООО «», (Приложение А).

Проведение контрольных мероприятий фиксируется в «Журнале учета внутренних проверок соблюдения режима безопасности при обработке персональных данных» (Приложение Б).

Контроль за эффективностью применяемых в ООО «» мер и средств защиты информации (далее – СЗИ) должен проводиться в соответствии с требованиями эксплуатационной документации на сертифицированные СЗИ, других нормативных документов, но не реже одного раза в год.

Обязательным является контроль за СЗИ при вводе их в эксплуатацию, после проведения ремонта, при изменении условий их расположения или эксплуатации.

В целях осуществления контроля соответствия обработки персональных данных (далее – ПДн) установленным требованиям в ООО «» организуется проведение периодических проверок условий обработки ПДн. Проверки осуществляются сотрудником, ответственным за обеспечение безопасности ПДн, либо комиссией, образуемой директором ООО «» не реже одного раза в год.

При осуществлении контроля соответствия обработки ПДн установленным требованиям производится проверка:

- соблюдения принципов обработки ПДн в ООО «»;

- соответствия организационно-распорядительной документации, регламентирующей обработку и обеспечение безопасности ПДн в ООО «», действующему законодательству Российской Федерации;

- выполнения сотрудниками ООО «» требований организационно-распорядительной документации, регламентирующей обработку ПДн и действующего законодательства Российской Федерации, включая обеспечение безопасности ПДн в информационной системе персональных данных (далее – ИСПДн);

- наличие актуального перечня ПДн, используемых для решения задач и функций структурными подразделениями ООО «» и необходимости обработки персональных данных в ИСПДн;

- актуальность перечня должностей сотрудников ООО «», замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;

- соблюдение прав субъектов ПДн, чьи персональные данные обрабатываются в информационных системах персональных данных ООО «»;

- порядка взаимодействия с субъектами ПДн, чьи персональные данные обрабатываются в ИСПДн ООО «», в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований по уведомлениям, порядка разъяснения субъектам ПДн необходимой информации, порядка реагирования на обращения субъектов ПДн, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами ПДн;

- наличие необходимых согласий субъектов ПДн, чьи персональные данные обрабатываются в ИСПДн ООО «»;

- актуальность сведений, содержащихся в уведомлении субъектов ПДн об обработке персональных данных в ООО «»;

- наличие и актуальность сведений, содержащихся в Положении об обработке ПДн в ООО «»;

- соблюдение сотрудниками ООО «» конфиденциальности ПДн;

- иных вопросов.

После окончания проверки, ответственный за обеспечение безопасности ИСПДн ООО «», либо председатель комиссии, представляет директору ООО «» отчет о результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений.

1. **Внешний контроль**

Внешний контроль соблюдения требований соблюдения законодательства Российской Федерации в области обеспечения безопасности при обработке ПДн в ИСПДн и без использования автоматизированной обработки, а также требований по защите ПДн, осуществляется комиссиями инспекции ФСТЭК России и Роскомнадзора. При проведении контрольных мероприятий комиссии инспекций ФСТЭК России и Роскомнадзора могут привлекать экспертов.

Проведение проверок комиссиями инспекций ФСТЭК России и Роскомнадзора осуществляется на основании плана проверок или в случае внеплановой проверки, на основании обращения субъекта ПДн или в случае выявления нарушений, допущенных ООО «» при обработке ПДн.

Проверки, осуществляемые комиссиями инспекций ФСТЭК России и Роскомнадзора фиксируется в «Журнале учета проверок ООО «», проводимых органами государственного контроля (надзора)» (Приложение Б).

**Приложение А**

(обязательное)

**Форма плана проведения внутренних контрольных мероприятий (проверок соблюдения требований по защите персональных данных) в ООО «»**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | УТВЕРЖДаЮ | | Директор ООО «» | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_ | | «\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. |   **План проведения внутренних контрольных мероприятий (проверок соблюдения требований по защите персональных данных) в ООО «»**   | № п.п. | Наименование контрольного мероприятия | Плановая дата проведения проверки | Дата проведения проверки | Фамилия инициалы проверяющего | Выявленные нарушения | Примечания | | --- | --- | --- | --- | --- | --- | --- | |  | Соблюдение принципов обработки ПДн в ООО «» |  |  |  |  |  | |  | Соответствие организационно-распорядительной документации, регламентирующей обработку и обеспечение безопасности ПДн в ООО «», действующему законодательству Российской Федерации |  |  |  |  |  | |  | Выполнение сотрудниками ООО «» требований организационно-распорядительной документации, регламентирующей обработку ПДн и действующего законодательства Российской Федерации, включая обеспечение безопасности ПДн в ИС «» |  |  |  |  |  | |  | Наличие актуального перечня ПДн, используемого для решения задач и функций структурными подразделениями ООО «» и необходимости обработки ПДн в ИСПДн АС «ТК» |  |  |  |  |  | |  | Актуальность перечня должностей сотрудников ООО «», замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн |  |  |  |  |  | |  | Соблюдение прав субъектов ПДн, чьи ПДн обрабатываются в ИС «» |  |  |  |  |  | |  | Порядок взаимодействия с субъектами ПДн, чьи ПДн обрабатываются в ИСПДн ООО «», в том числе соблюдения сроков, предусмотренных действующим законодательством в области ПДн, соблюдения требований по уведомлениям, порядка разъяснения субъектам ПДн необходимой информации, порядка реагирования на обращения субъектов ПДн, порядка действий при достижении целей обработки ПДн и отзыве согласий субъектами ПДн |  |  |  |  |  | |  | Наличие согласий субъектов ПДн, чьи ПДн обрабатываются в ИС «» |  |  |  |  |  | |  | Актуальность сведений, содержащихся в уведомлении субъектов ПДн об обработке ПДн в ООО «» |  |  |  |  |  | |  | Наличие и актуальность сведений, содержащихся в Положении об обработке ПДн в ООО «» |  |  |  |  |  | |  | Соблюдение сотрудниками ООО «» конфиденциальности ПДн |  |  |  |  |  | |  | Представление отчета директору ООО «» |  |  |  |  |  | |

**Приложение Б**

(обязательное)

**Форма журнала учета внутренних проверок соблюдения режима безопасности при обработке персональных данных**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Журнал учета внутренних проверок соблюдения режима безопасности при обработке персональных данных**   |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **№**  **п/п** | **Наименование проверки** | **Краткое описание проверки** | **Наименование подразделения, в котором проводилась проверка** | **Дата проведения проверки** | **Результат проверки** | **Фамилия И.О.**  **лица (лиц), проводившего**  **проверку** | **Подпись лица (лиц),**  **проводившего**  **проверку** | **Примечание** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |   Страница 1 из \_\_\_ |

**Приложение В**

(обязательное)

**Форма журнала учета проверок ООО «», проводимых органами государственного контроля (надзора)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Журнал учета проверок ООО «», проводимых органами государственного контроля (надзора)**   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **№**  **п/п** | **Наименование проверки** | **Краткое описание проверки** | **Наименование органа, проводившего проверку** | **Основания для проведения проверки (номер и дата приказа/ распоряжения)** | **Дата**  **проведения**  **проверки** | **Результат проверки** | **Фамилия И.О.**  **лица (лиц), проводившего**  **проверку** | **Подпись лица (лиц),**  **проводившего**  **проверку** | **Примечание** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |   Страница 1 из \_\_\_ |