

АКТ ОБСЛЕДОВАНИЯ

системы защиты персональных данных в муниципальном дошкольном бюджетном образовательном учреждении «Детский сад №56»

28 июня 2019 года в соответствии с договором от 1 марта 2019 года № 208-19030131 специалистами ИП Ларионов И.Е. проведено обследование организации обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационной системе персональных данных (далее – ИСПДн), на соответствие требованиям ФЗ-№152 от 27 июля 2006 года «О персональных данных», ФЗ-№149 от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации», постановления Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», постановления Правительства РФ от 21 марта 2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», руководящего документа «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденного приказом Гостехкомиссии России от 30 августа 2002 г. № 282».

Для определения соответствия системы информационной безопасности организации требованиям вышеперечисленных нормативно-правовых актов необходимо определить:

1. Состав информационной системы персональных данных;
2. Структуру информационной системы персональных данных;
3. Состав, объем и режимы обработки персональных данных;
4. Права доступа лиц, допущенных к обработке персональных данных;
5. Существующие меры защиты персональных данных.

Данные проведенного обследования служат информационной основой для внутренних нормативно-организационных документов организации, а именно:

1. Данные о составе и структуре ИСПДн и существующие меры защиты персональных данных служат основой для составления Модели угроз безопасности персональных данных.

2. Состав и объем обрабатываемых ПДн служат основой для составления Акта классификации ИСПДн и перечня персональных данных подлежащих защите.

1. Сведения об информационных системах персональных данных

В ходе обследования системы защиты персональных данных в муниципальном дошкольном бюджетном образовательном учреждении «Детский сад №56» (далее – Детский сад) были выявлены следующие информационные системы персональных данных:

1. «АРМ заведующего»
2. «Сайт»

1.1. Описание информационной системы «АРМ заведующего»

Информационная система развёрнута на одном компьютере. Компьютер имеет выход в сеть Интернет. Обработка персональных данных осуществляется в программах «Microsoft Office», «Spu_orb», «Заполнение форм статистической отчетности», «СПО «Справки БК», веб-портале «Сетевой город. Образование». Персональные данные передаются в Управление образования администрации Красноармейского района, МКУ «Укрупненная централизованная бухгалтерия при управлении образования» администрации Красноармейского района, ГКУ Краснодарского края «Центр занятости населения Красноармейского района», Управление социальной защиты населения министерства труда и социального развития Краснодарского края в Красноармейском районе, Управление Пенсионного фонда России Красноармейского района Краснодарского края, ГБУЗ «Красноармейская центральная районная больница» электронной почтой, на бумажных носителях, на флэшке, нарочным.

1.1.1. Объекты защиты

– Средства обработки информации (персональные компьютеры);

– Персональные данные:

1. Фамилия, имя, отчество
2. Тип документа, удостоверяющего личность, серия и номер, дата выдачи
3. Дата рождения
4. Адрес места жительства/прописки
5. Идентификационный номер налогоплательщика (ИНН)
6. Страховой номер индивидуального лицевого счета (СНИЛС)
7. Номер телефона
8. Адрес электронной почты
9. Семейное положение
10. Образование, категория, квалификация, звание
11. Профессия
12. Должность
13. Стаж

14. Сведения о доходах
15. Сведения о воинской обязанности и военной службе
16. Сведения об имуществе
17. Реквизиты лицевых счетов, банковских карт

1.1.2. Количество записей о субъектах персональных данных

В информационной системе персональных данных обрабатывается менее 100 000 записей, содержащих данные о субъектах персональных данных.

1.1.3. Должностные лица, имеющие доступ к работе с информационной системой

1. Заведующий

1.1.4. Режимы обработки персональных данных

1. Сбор
2. Хранение
3. Обработка
4. Передача

1.1.5. Уровень защищенности информационной системы

В соответствии с постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», исходя из того, что в информационной системе обрабатываются иные категории ПДн сотрудников организации и субъектов, не являющихся сотрудниками организации, в количестве менее 100 000 субъектов ПДн и для информационной системы актуальны угрозы 3-го типа, информационной системе необходимо обеспечить 4 уровень защищенности.

1.1.6. Установленные средства защиты информации

1. Avast Free Antivirus

1.2. Описание информационной системы «Сайт»

Информационная система представляет собой официальный сайт Детского сада с доменным именем <https://dou56kr.myl.ru>. Общедоступная информация о деятельности Детского сада в соответствии с Правилами размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации, утвержденными Постановлением Правительства России от 10 июля 2013 г. № 582, предоставляется неограниченному кругу лиц посредством ее размещения в сети Интернет в форме открытых данных на официальном сайте Детского сада. Сайт размещен на виртуальном хостинге, датацентр расположен на территории Российской Федерации в городе Москва. На сайте используется безопасный протокол HTTPS, что исключает возможность перехвата сессии легального пользователя и проведения атаки «человек посередине».

1.2.1. Объекты защиты

– Средства обработки информации (персональные компьютеры);

– Персональные данные:

1. Фамилия, имя, отчество
2. Должность
3. Номер телефона
4. Адрес электронной почты
5. Образование
6. Стаж

1.2.2. Количество записей о субъектах персональных данных

В информационной системе персональных данных обрабатывается менее 100 000 записей, содержащих данные о субъектах персональных данных.

1.2.3. Должностные лица, имеющие доступ к работе с информационной системой

1. Воспитатель

1.2.4. Режимы обработки персональных данных

1. Сбор
2. Хранение
3. Обработка
4. Передача

1.2.5. Уровень защищенности информационной системы

В соответствии с постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», исходя из того, что в информационной системе обрабатываются иные категории ПДн сотрудников организации и субъектов, не являющихся сотрудниками организации, в количестве менее 100 000 субъектов ПДн и для информационной системы актуальны угрозы 3-го типа, информационной системе необходимо обеспечить 4 уровень защищенности.

1.2.6. Установленные средства защиты информации

1. Резервное копирование
2. Включена защита от DDOS-атак
3. Включена защита сессий
4. Включена защита редиректов от фишинга
5. Включена защиты от фреймов
6. Включен контроль активности
7. Включен журнал событий

2. Сведения о документах, содержащих персональные данные

В Детском саду имеются документы, содержащие персональные данные (личные дела сотрудников, трудовые книжки, трудовые договоры, личные дела детей, приказы по основной деятельности и по личному составу, медицинские книжки сотрудников, медицинские карточки детей). Перечисленные документы хранятся в следующих местах:

1. Личные дела сотрудников в запираемом кабинете.
2. Трудовые книжки в сейфе.
3. Трудовые договоры в запираемом кабинете.
4. Личные дела детей в запираемом кабинете.
5. Приказы по основной деятельности и по личному составу в запираемом кабинете.
6. Медицинские книжки сотрудников в запираемом кабинете.
7. Медицинские карточки детей в запираемом кабинете.

В соответствии с п. 15 Постановления Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» перечень мер защиты от несанкционированного доступа к материальным носителям определяется оператором.

Предпринятые меры являются достаточными.

3. Результаты обследования

В соответствии со ст. 18.1, ст. 19 п. 1 ФЗ-152 от 27 июля 2006 года «О персональных данных», ст. 16 п. 1 ФЗ-149 «Об информации, информатизации и о защите информации» для защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации необходимо принятие правовых, организационных и технических мер.

Для реализации вышеперечисленных требований, в соответствии с п. 3.18 СТР-К, постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 рекомендуется разработать следующие организационно-распорядительные документы, которые регламентируют порядок доступа к персональным данным, правила работы с персональными данными и порядок работы со средствами защиты информации, а именно:

1. Инструкцию системного администратора информационных систем персональных данных по обеспечению безопасности персональных данных;
2. Инструкцию о порядке резервирования и восстановления работоспособности технических средств, программного обеспечения и баз данных;
3. Инструкцию ответственного за обработку персональных данных;
4. Инструкцию по организации антивирусной защиты;
5. Инструкцию по порядку учета и хранению документов, содержащих персональные данные;
6. Инструкцию по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ);
7. Инструкцию по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных);
8. Инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных;
9. Положение об обработке персональных данных;
10. Порядок доступа сотрудников в помещения, где ведётся обработка персональных данных;
11. Приказ о назначении администраторов информационных систем и ответственных за обработку персональных данных;
12. Приказ о классификации информационных систем;
13. Акты классификации информационных систем;
14. Приказ о вводе в эксплуатацию информационных систем;
15. Частную модель угроз безопасности ПДн;

16. Разрешительную систему доступа к информационным системам;

17. Перечень должностей сотрудников, имеющих доступ к работе с персональными данными.

Также, наряду с организационными мерами, на основании постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», для обеспечения

4 уровня защищённости необходимо выполнить следующие требования:

Организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

Обеспечение сохранности носителей персональных данных

Утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей

Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз

Также сообщаем вам, что необходимо уничтожить все копии документов, удостоверяющих личность (паспорт), если их хранение не предусмотрено действующим законодательством.