Персональные данные

Совещание 12.03.2014

Пимкина Г.И.
МбОУ лицей №4

МИНИСТЕРСТВО ОБРАЗОВАНИЯ
МОСКОВСКОЙ ОБЛАСТИ

бульвар Строителей, д. 1, г. Красногорск-7, Московская область, 143407
пр. Юбилейный, д. 59, г. Химки, Московская область, 141400
тел. 8 (498) 602-11-11; факс 8 (498) 602-09-93
e-mail: minobr@mosreg.ru; minomos@mail.ru

10.01.2014 № Исх-492/06 дл

На № _____ от _____

Руководителям муниципальных
органов управления образованием
Московской области

Министерство образования Московской области (далее - Министерство) сообщает, что в июне этого года Федеральной службой по техническому и экспортному контролю России запланирована проверка Московской области, в частности государственных учреждений, по вопросам информационной безопасности.

В целях совершенствования защиты информационных систем персональных данных прошу:

1. Провести всесторонний анализ состояния защиты персональных данных граждан при их обработке с использованием средств автоматизации и без использования таких средств.
2. Уточнить, при необходимости переработать потерявшую актуальность организационно-распорядительную документацию, регламентирующую порядок обработки персональных данных.

Министр образования
Московской области Захарова М.Б. Захарова

АДМИНИСТРАЦИЯ
КРАСНОГОРСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
МОСКОВСКОЙ ОБЛАСТИ

УПРАВЛЕНИЕ ОБРАЗОВАНИЯ

143403, Московская область,
г.Красногорск, ул. Кирова, д. 7 А
тел.: 563-89-46, 564-71-32
E-mail: obrkrasn@yandex.ru

от ___24.02.2014___№__181_____

на №_____от_____

Руководителям
общеобразовательных
учреждений

Управление образования Красногорского муниципального района в соответствии с письмом Министерства образования Московской области №492/06и от 10.02.2014 сообщает, что в июне этого года Федеральной службой по техническому и экспортному контролю России запланирована проверка Московской области, в частности государственных учреждений, по вопросам информационной безопасности.

В целях совершенствования защиты информационных систем персональных данных необходимо:

1. Провести всесторонний анализ состояния защиты персональных данных граждан при их обработке с использованием средств автоматизации и без использования таких средств.
2. Уточнить, при необходимости переработать потерявшую актуальность организационно-распорядительную документацию, регламентирующую порядок обработки персональных данных

Начальник Управления образования Т. В. Швейниц

исп. Пимкина Г. И.
тел. 563-63-34

Организация работ по построению системы защиты информации – это содержание и порядок действий по обеспечению защиты информации, организованных по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Организация работ по защите информации возлагается на руководителей организации.

Методическое руководство и контроль за эффективностью предусмотренных мер защиты информации возлагается на ответственного за защиту информации.

Защита ИСПДн в школах достигается проведением комплекса организационно-распорядительных мероприятий:

1. Подбор специалиста по защите информации из числа сотрудников.
2. Определение перечня информационных систем персональных данных (далее - ИСПДн).
3. Проведение классификации этих систем по требованиям безопасности информации.
4. Разработка комплекта документов на ИСПДн.
5. Наличие на всех компьютерах только лицензионного программного обеспечения.
6. Построение системы защиты ИСПДн.

Комплект документов на ИСПДн

1. ПРИКАЗ «Об организации работ по защите ПДн в учреждении»
2. ПОЛОЖЕНИЕ по обработке и защите ПДн
3. ПЕРЕЧЕНЬ ПДн, обрабатываемых в школе
4. ПЕРЕЧЕНЬ ИСПДн в учреждении
5. ПЕРЕЧЕНЬ сотрудников, имеющих право доступа к ИСПДн
6. АКТЫ классификации ИСПДн
7. МОДЕЛЬ угроз безопасности ПДн, обрабатываемых в ИСПДн
8. ИНСТРУКЦИЯ по работе пользователей ИСПДн
9. ИНСТРУКЦИЯ ответственного
10. ЖУРНАЛ учёта паролей
11. ЖУРНАЛ учёта машинных носителей информации

1. Управления доступом:

идентификация и проверка подлинности пользователя при входе в ИСПДн по паролю длиной не менее шести символов

2. Регистрации и учета:

- регистрация и учёт входа (выхода) пользователя в систему;
- учёт всех защищаемых носителей информации

3. Обеспечения целостности:

- обеспечение целостности программных средств СЗ ПДн;
- физическая охрана ИСПДн и носителей информации;
- периодическое тестирование СЗ ПДн;
- наличие средств восстановления СЗ ПДн

* http://pdn2.com/registers/dannie

на № 827 от 26.08.2013 года
Об обработке персональных данных.
Исх. 723 от 27.08. 2013года.

Наименование учреждения	Правовое основание обработки персональных данных	Наименование юридического лица, ответственного за организацию обработки персональных данных, номера контактных телефонов, почтовые адреса и адреса электронной почты	Сведения о наличии или отсутствии трансграничной передачи персональных данных в процессе их обработки	Сведения об обеспечении безопасности персональных данных
Муниципальное бюджетное общеобразовательное учреждение «Нахабинская гимназия № 4»	Трудовой кодекс Российской Федерации ст. 85-90. Положение об обработке персональных данных в МБОУ «Нахабинская гимназия № 4» Пр. от 25.03.2013г. № 193. Ст. 6. ФЗ от 27.07.2006г. № 152 «Оперсональных данных».	Директор гимназии Садовская Татьяна Владимировна тел. 8-495-566-20-00 143433 Московская обл. Красногорский р-он г.п. Нахабино ул., Школьная д. 6. gim465@yadex.ru	нет	Разграничение прав доступа сотрудников к базе ПДн. Наличие Положения и Инструкции об обработке ПДн. Обеспечение охраны помещений с базами ПДн информации на магнитных и бумажных носителях, а также специально выделенной сети. Наличие сейфа, шкафа(запирающихся на ключ) для хранения носителей информации с ПДн. Наличие антивирусного программного обеспечения. Сигнализация. Видеонаблюдение.

Директор
МБОУ «Нахабинская гимназия № 4» Т.В. Садовская

Приказ о проведении внутренней проверки

В Приказе должен быть установлен срок, до которого необходимо провести внутреннюю проверку. Проверка проводится на основании Приказа о проведении внутренней проверки.

В приказе должен быть указан сотрудник, ответственный за контроль исполнения приказа. Ответственным сотрудником может быть Руководитель Учреждения, лицо, отвечающее за обеспечение режима безопасности, или любой другой сотрудник, на которого возложен контроль за выполнение приказа

При проверке Роскомнадзор проверяет все документы, представленные в Приложении.
Минимальный набор включает: отчет по результатам внутренней проверки, модель угроз для каждой ИСПДн, акт классификации для каждой ИСПДн.

1.1 Общие рекомендации

Для успешного прохождения проверки о соблюдении законодательства в области персональных данных необходимо следующее.

Ежегодно в начале года проверять наличие Учреждения в Сводном плане проверок субъектов предпринимательства на сайте Генеральной Прокуратуры (план на 2010 год – http://79.125.23.79/) и Плане проведения плановых проверок Роскомнадзора (план на 2010 год – http://rkn.gov.ru/plan-and-reports/contolplan/

Утвердить в соответствии с внутренними требованиями документооборота необходимые документы для обеспечения режима безопасности персональных данных (далее – ПДн):

- учредительные документы Оператора;
- копия уведомления об обработке персональных данных;
- положение о порядке обработки персональных данных;
- положение о подразделении, осуществляющем функции по организации защиты персональных данных;

должностные регламенты лиц, имеющих доступ к персональным данным (пользователя, администратора, администратора безопасности);

– план мероприятий по защите персональных данных;

– план внутренних проверок состояния защиты персональных данных;

– приказ о назначении ответственных лиц по работе с персональными данными;

– типовые формы документов, предполагающие или допускающие содержание персональных данных;

– журналы, реестры, книги, содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях;

договоры с субъектами персональных данных, лицензии на виды деятельности, в рамках которых осуществляется обработка персональных данных;

выписки из ЕГРЮЛ, содержащие актуальные данные на момент проведения мероприятия по контролю (надзору);

приказы об утверждении мест хранения материальных носителей персональных данных;

письменное согласие субъектов персональных данных на обработку их персональных данных (типовая форма);

распечатки электронных шаблонов полей, содержащие персональные данные;

справки о постановке на балансовый учет ПЭВМ, на которых осуществляется обработка персональных данных;

заключения экспертизы ФСБ России, ФСТЭК России об оценке соответствия средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке (проверяется только наличие данных документов) или декларацию соответствия;

приказ о создании комиссии и акты классификации ИСПДн (проверяется только наличие данных документов);

журналы (книги) учета обращений граждан (субъектов персональных данных);

акт об уничтожении персональных данных субъекта(ов) персональных данных (в случае достижения цели обработки);

иные документы, отражающие исполнение Оператором требований законодательства Российской Федерации в области персональных данных.

Дополнительными, часто запрашиваемыми документами, могут являться:

– электронный журнал обращений пользователей информационной системы к ПДн;

– эксплуатационная и техническая документация (техническое задание, технорабочий проект, паспорт автоматизированной системы);

– отражение в трудовом договоре (контракте) ответственности работника за разглашение ПДн;

– Концепция информационной безопасности;

– Политика информационной безопасности;

порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ

Поддерживать в актуальном состоянии введенные меры обеспечения безопасности персональных данных (организационные и технические), вести установленным порядком необходимые журналы, а так же на периодической основе (не реже 2 раз в год) осуществлять контролирующие мероприятия за соблюдением действующего режима безопасности.

Для всех новых информационных систем должно быть определено наличие принадлежности к множеству информационных систем персональных данных (ИСПДн). Если в системе производится обработка персональных данных, то для каждой новой ИСПДн необходимо:

– создать коллегиальный орган из сотрудников Учреждения (подразделения ИБ, IT, структурных подразделений эксплуатирующих ИСПДн) или заключить договор с лицензиатом ФСТЭК России для реализации дальнейших шагов;

определить назначение новой ИСПДн и круг лиц, работающих с данной ИСПДн;

– классифицировать новую ИСПДн в соответствии с Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности (ФСБ России), Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

– создать (описать) модель угроз для каждой новой ИСПДн и описать средства защиты;

– определить необходимость уведомления Роскомнадзора о наличии ИСПДн, и подать такое уведомление в случае необходимости;

обеспечить техническими и организационными мерами требуемый уровень безопасности для каждой новой ИСПДн в соответствии с ее классом;

– при необходимости сертифицировать систему защиты ИСПДн или саму ИСПДн во ФСТЭК России, получить лицензию на деятельность по технической защите.

В случае, если Учреждение попало в Сводный план проверок субъектов предпринимательства и/или План проведения плановых проверок Роскомнадзора, необходимо выяснить в проверяющем органе предполагаемую дату проверки.

Плановая проверка может быть проведена 1 раз в 3 года.

В случае, если Учреждение уведомило Роскомнадзор о том, что оно является оператором персональных данных, она будет планово проверена Роскомнадзором в течение трех лет.

– В случае, если Учреждение проверяется внепланово, она должна быть заранее уведомлена контролирующим органом за 3 дня. В случае отсутствия уведомления проверка считается нелегитимной.

1.1 Рекомендации в случае прихода проверки

В случае, если Учреждение получило уведомление о проведении проверки необходимо:

– проверить правильность заполнения всех необходимых журналов;

– собрать комплект необходимых документов, что бы он был в оперативной готовности;

– проинструктировать работников основных структурных подразделений, работающих с ИСПДн Учреждения, о порядке работы и защиты персональных данных;

– организовать оперативный просмотр электронных журналов обращений пользователей информационных систем к ПДн, а так же журналов средств защиты информации и другим формам учета;

определить ответственного сотрудника, который будет сопровождать проверяющих.

Подведение итогов

Итак, в организации для работы с персональными данными должны быть следующие документы:

1. Положение о персональных данных.
2. Приказ о назначении ответственных за работу с персональными данными.
3. Приказ о назначении ответственных за обеспечение безопасности персональных данных.
4. Заявления работников на обработку персональных данных.
5. Договоры (допсоглашения) с работниками об обработке персональных данных