Русская Академия Ремёсел
Некоммерческое образовательное частное учреждение дополнительного профессионального образования
Свидетельство Министерства юстиции РФ 7714041778 от 13.11.2013 г. Лицензия Департамента образования города Москвы № 037362 от 11.04.2016 г.

Исх.№ _____ от _____201___г.

«УТВЕРЖДАЮ»
Ректор

НОЧУ ДПО «РАР»
Просвирина Е.А.

«30» октября 2018 г.

МЕТОДИКА ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

Москва, 2018

Содержание

1 Общие положения **3**
2 Методические рекомендации **4**
2.1 Общие сведения 4
2.2 Общие требования к организации контрольных мероприятий 4
2.3 Планирование контрольных мероприятий 6
2.4 Состав контрольных мероприятий 6
2.4.1 Оценка компетентности работников, задействованных в обработке персональных данных 6
2.4.2 Проверка работоспособности технических средств информационных систем персональных данных и средств защиты персональных данных 7
2.4.3 Проверка соответствия прав доступа к персональным данным утвержденной матрице доступа 7
2.4.4 Проверка выполнения требований парольной политики 7
2.4.5 Проверка отсутствия на автоматизированных рабочих местах пользователей нештатного программного обеспечения и средств разработки 8
2.4.6 Периодическое тестирование функций системы защиты 8
2.4.7 Проверка правильности ведения учета носителей персональных данных 9
2.4.8 Проверка работоспособности резервных копий 9
2.4.9 Проверка работ по приему и обработке обращений субъектов персональных данных и уполномоченного органа по защите прав субъектов персональных данных 9
2.4.10 Разработка и принятие корректирующих мер, направленных на устранение выявленных нарушений 10
Приложение А Форма Приказа о назначении комиссии по контролю соответствия принятых мер защиты персональных данных **11**
Приложение Б Проект плана контроля соответствия принятых мер защиты персональных данных **12**
Приложение В Форма Журнала учета выявленных нарушений в обеспечении безопасности персональных данных **16**
Приложение Г Форма Протокола о результатах проведения проверки **17**

Общие положения

- Настоящий документ содержит Методику эксплуатации информационных систем персональных данных в государственных образовательных учреждениях, подведомственных Департаменту образования города Москвы (далее – Методика).
- Настоящая Методика учитывает требования к организации порядка обработки персональных данных в соответствии с действующим законодательством Российской Федерации о персональных данных.

- **Методические рекомендации**
- **Общие сведения**

В соответствии с требованиями статьи 18.1 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» каждый оператор персональных данных должен осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных указанного федерального закона и принятым в соответствии с ним нормативным правовым актам требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

Контроль выполнения требований документа «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации от 01.11.2012 г. №1119, организуется и проводится оператором самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации, не реже 1 раза в 3 года.

Методическую базу для проектирования системы защиты персональных данных при их обработке в информационных системах персональных данных составляют следующие документы:

- Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства Российской Федерации от 01.11.2012 г. №1119.

- **Общие требования к организации контрольных мероприятий**

Организация внутреннего контроля порядка обработки персональных данных в образовательной организации (далее – ОО) осуществляется в соответствии с

локальным актом ОО «Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке».

В соответствии с указанным документом мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности персональных данных направлены на решение следующих задач:

- обеспечение соблюдения работниками ОО требований локальных документов ОО и нормативных правовых актов, регулирующих защиту персональных данных;
- оценка компетентности работников, задействованных в обработке персональных данных;
- обеспечение работоспособности и эффективности технических средств информационных систем персональных данных и средств защиты персональных данных, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности персональных данных;
- выявление нарушений установленного порядка обработки персональных данных и своевременное предотвращение негативных последствий таких нарушений;
- принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки персональных данных, так и в работе технических средств информационных систем персональных данных;
- разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности персональных данных по результатам контрольных мероприятий;
- осуществление контроля исполнения рекомендаций и указаний по устранению нарушений.

Контрольные мероприятия организуются Ответственным за организацию обработки персональных данных.

Для проведения контрольных мероприятий приказом директора ОО созывается комиссия по контролю соответствия принятых мер защиты персональных данных

(Приложение А). В состав комиссии обязательно должны входить Ответственный за организацию обработки персональных данных, Ответственный за обеспечение безопасности персональных данных (если такое лицо назначено), представители администрации ОО, работники, осуществляющие администрирование информационной инфраструктуры ОО.

- **Планирование контрольных мероприятий**

Контрольные мероприятия включают в себя задачи с разной периодичностью выполнения. Планирование контрольных мероприятий должно учитывать необходимую периодичность повторных проверок.

Проект плана контроля (Приложение Б) содержит рекомендованные сроки проведения проверок и подлежит уточнению по результатам оценки комиссией по контролю соответствия, в том числе назначению конкретных временных промежутков проведения проверок в зависимости от производственных процессов ОО. Уточнение плана контроля может проводиться перед проведением проверки, а также при выявлении такой необходимости.

- **Состав контрольных мероприятий**

- ***Оценка компетентности работников, задействованных в обработке персональных данных***

Оценку компетентности работников, задействованных в обработке персональных данных, необходимо осуществлять не реже, чем один раз в три года, а для принимаемых новых работников – до предоставления доступа к персональным данным.

Оценка проводится в формате тестирования, включающего в себя вопросы по требованиям, содержащимся в локальных нормативных актах ОО и законодательстве, и ситуационные задачи, связанные непосредственно со служебными обязанностями тестируемого работника, с которыми работник потенциально может встретиться при участии в производственных процессах ОО.

Опросники составляются Ответственным за организацию обработки персональных данных с учетом ситуаций, встречавшихся в производственных

процессах ОО, выявленных инцидентов нарушения безопасности персональных данных. Использование при тестировании задач, прямо применимых в деятельности работника, позволяет оценить степень компетентности работника и понимания им сути требований нормативных документов.

- ***Проверка работоспособности технических средств информационных систем персональных данных и средств защиты персональных данных***

Проверка работоспособности технических средств и средств защиты персональных данных осуществляется для выявления сбоев в их работе, которые сложно заметить в ходе выполнения рабочего процесса, в частности, когда отключение каких-либо защитных функций не отражается на деятельности пользователя, но увеличивает вероятность реализации угроз безопасности персональных данных.

Кроме того, в рамках проверки работоспособности осуществляется контроль установки обновлений программного обеспечения: настройки автоматического обновления, сведения журналов учета установки новых версий, используемые версии.

- ***Проверка соответствия прав доступа к персональным данным утвержденной матрице доступа***

В ОО должен быть утвержден список лиц, доступ которых к персональным данным необходим для выполнения служебных обязанностей. В ходе контроля соответствия прав доступа следует проверить, что в каждой из групп доступа находятся только те лица, доступ которых санкционирован. Если в проверяемых компонентах консолидированная выгрузка сведений о пользователях и их допусках не поддерживается, следует проверить каждую локальную запись вручную.

- ***Проверка выполнения требований парольной политики***

В ходе проверки выполнения требований парольной политики проверяются конфигурации системного и прикладного программного обеспечения на соответствие требованиям парольной политики или следующим минимальным требованиям: длина пароля не менее 6 буквенно-цифровых знаков и спецсимволов,

буквенные знаки разных регистров. Рекомендуется, чтобы парольная политика была зафиксирована в виде соответствующего локального акта ОО.

- ***Проверка отсутствия на автоматизированных рабочих местах пользователей нештатного программного обеспечения и средств разработки***

На автоматизированных рабочих местах пользователей должно быть установлено только программное обеспечение, необходимое пользователям для выполнения служебных обязанностей. Возможность установки любого другого программного обеспечения должна быть исключена, у пользователей не должно быть прав, позволяющих изменять состав программного обеспечения.

Если проверка осуществляется вручную, то следует проводить ее по случайной выборке, составляющей не менее 10% из общего количества автоматизированных рабочих мест. Если проверка осуществляется с помощью специализированных инструментов, то проверке должны подвергаться все автоматизированные рабочие места.

- ***Периодическое тестирование функций системы защиты***

Тестирование функций системы защиты, как правило, выполняется с помощью инструментальных средств анализа защищенности, выполняющих как нагрузочное тестирование и имитацию действий нарушителя, так и проверку корректности настроек встроенных функций обеспечения безопасности, средств защиты, наличия известных уязвимостей в установленных версиях программного обеспечения.

В случае проведения тестирования без применения специализированных инструментальных средств по общедоступным источникам проверяется:

- наличие уязвимостей в программном обеспечении;
- методы противодействия использованию уязвимостей злоумышленником;
- эффективность используемых конфигураций программного обеспечения и средств защиты в соответствии с лучшими практиками и рекомендациями поставщиков средств;
- соответствие используемых конфигураций программного обеспечения и средств защиты формулярам и эксплуатационной документации на эти средства.

- ***Проверка правильности ведения учета носителей персональных данных***

К защищаемым носителям персональных данных относятся:

- носители информации серверов;
- носители информации автоматизированных рабочих мест;
- внешние запоминающие устройства: флеш-накопители, внешние жесткие диски, карты памяти, компакт-диски и др.

Каждый носитель, который используется для хранения персональных данных, должен быть промаркирован и внесен в Журнал учета. Во время проверки следует:

- проверить соответствие маркировок и внесенной в Журнал информации по всем носителям, установленным на серверах;
- проверить соответствие маркировок и внесенной в Журнал информации по носителям, установленным на автоматизированных рабочих местах;
- проверить наличие маркировок на съемных носителях, используемых работниками в процессе производственной деятельности, и соответствие внесенной в Журнал информации;
- для мобильных рабочих мест (ноутбуков, планшетов и др.), в которых нет доступа к устройству хранения, проверить инвентарный номер рабочего места и информацию, внесенную в Журнал учета носителей.

- ***Проверка работоспособности резервных копий***

Проверка работоспособности резервных копий заключается в тестовом восстановлении данных из хранящихся копий. В область оценки должны входить резервные копии различного срока хранения, созданные с момента предыдущей проверки.

- ***Проверка работ по приему и обработке обращений субъектов персональных данных и уполномоченного органа по защите прав субъектов персональных данных***

Проверку работ по приему и обработке обращений субъектов персональных данных и уполномоченного органа по защите прав субъектов персональных данных

(Роскомнадзор) осуществляет директор ОО, анализируя журналы фиксации обращений субъектов персональных данных и Роскомнадзора на предмет:

- корректности фиксации всей информации по обращению и ответам;
- соблюдения сроков предоставления ответа;
- соблюдения правовых оснований для ответа и отказа в предоставлении сведений.

- ***Разработка и принятие корректирующих мер, направленных на устранение выявленных нарушений***

По результатам проведения каждой из проверок составляется Протокол проведения проверки (Приложение Г), на основании которого заполняется Журнал учета выявленных нарушений (Приложение В) и формируется план действий, принятие которых необходимо для устранения выявленных нарушений.

По каждому из выявленных нарушений проводится анализ для установления причин появления нарушений и формирования перечня корректирующих мер. При необходимости следует провести служебное расследование.

Корректирующие меры выбираются таким образом, чтобы устранить нарушение или минимизировать его последствия, если полное устранение нарушения невозможно. Срок устранения нарушений устанавливается лицом, проводившим проверку, при этом срок не может превышать половины от общего времени, проходящего между проверками того типа, в ходе которых выявлено нарушение.

После устранения нарушения может быть проведена внеплановая повторная проверка.