СОГЛАСОВАНО:
Председатель первичной профсоюзной организации ГБОУ Лицея № 1580

_____ Игуменов А.А.

Протокол № 37 «21» марта 2018 г.

УТВЕРЖДЕНО:
Директор ГБОУ Лицея № 1580

_____ С.С. Граськин

Приказ № 142 от «21» марта 2018 г.

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в Государственном бюджетном общеобразовательном учреждении города Москвы «Лицей № 1580 при МГТУ имени Н.Э. Баумана»

1.Введение

1.1 Настоящее Положение разработано в соответствии с законодательством Российской Федерации о персональных данных и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности персональных данных, в том числе при их обработке в информационных системах персональных данных.

1.2 Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение, являются:

- Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), устанавливающий основные принципы и условия обработки персональных данных, права, обязанности и ответственность участников отношений, связанных с обработкой персональных данных;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.1 Для осуществления мероприятий по обеспечению и контролю безопасности персональных данных, обработки обращений субъектов персональных данных и взаимодействия с уполномоченным органом по защите прав субъектов персональных данных приказом директора Государственного бюджетного общеобразовательного учреждения города Москвы «Лицей № 1580 при МГТУ имени Н.Э. Баумана» (далее – образовательная организация) назначается работник, ответственный за организацию обработки персональных данных, и работник, ответственный за обеспечение безопасности персональных данных.

1.2 Настоящее Положение подлежит пересмотру и при необходимости актуализации в случае изменений в законодательстве Российской Федерации о персональных данных, при изменении организационной структуры образовательной организации.

2. Общие положения

2.1. Настоящее Положение предназначено для организации в образовательной организации процесса обеспечения безопасности персональных данных согласно требованиям действующего федерального законодательства.

2.2. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передаче), обезличиванию, блокированию, уничтожению персональных данных, осуществляемые с использованием средств автоматизации и без их использования.

2.3. Положение обязательно для ознакомления и исполнения работниками образовательной организации, являющимися ответственными за организацию обработки персональных данных и ответственными за обеспечение

безопасности персональных данных, инженерами по телекоммуникации (техниками).

3. Роли персонала

3.1. Во исполнение положений настоящего документа и соответствия требованиям законодательства Российской Федерации о персональных данных в образовательной организации введены следующие роли персонала:

- ответственный за организацию обработки персональных данных;
- ответственный за обеспечение безопасности персональных данных.

3.2. Назначение работников на роли ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных осуществляется приказом директора образовательной организации.

4. Обязательные мероприятия по обеспечению безопасности информационных систем персональных данных

4.1. В образовательной организации до начала проведения работ по обеспечению безопасности персональных данных должна быть проведена инвентаризация информационных систем персональных данных путем опроса владельцев информационных систем на предмет наличия обработки в них персональных данных.

4.2. После инвентаризации информационных систем выявляются информационные системы персональных данных, в которых осуществляется автоматизированная обработка персональных данных, и информационные системы персональных данных, в которых осуществляется неавтоматизированная обработка персональных данных.

4.3. Для всех эксплуатируемых информационных систем персональных данных с автоматизированной обработкой персональных данных должны быть определены уровни защищенности персональных данных в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 г.

№ 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.4. По согласованию с Департаментом образования города Москвы в образовательных организациях могут использоваться собственные информационные системы персональных данных. Порядок ввода в эксплуатацию и вывода из эксплуатации таких информационных систем описаны в приложении Ж.

4.5. В случае создания новых информационных систем персональных данных, расширения состава данных в существующих информационных системах персональных данных, модернизации информационных систем персональных данных определение уровня защищенности персональных данных проводится в следующей последовательности:

а) на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) приказом директора образовательной организации создается Комиссия по проведению определения уровней защищенности персональных данных в информационных системах персональных данных;

б) Комиссия в определенный приказом срок устанавливает категории, принадлежность и объем обрабатываемых персональных данных в информационных системах персональных данных, а также определяет тип актуальных для информационных систем персональных данных угроз безопасности персональных данных, связанных с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении;

в) Комиссия формирует акты определения уровней защищенности персональных данных для каждой информационной системы персональных данных, в которых указываются типы угроз безопасности персональных данных в информационных системах персональных данных, перечень обрабатываемых категорий персональных данных, их принадлежность и количество записей, содержащих персональные данные.

4.6. В образовательной организации должны быть разработаны модели угроз безопасности персональных данных для всех информационных систем персональных данных. Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с ч. 5 ст. 19 Закона о персональных данных.

4.7. Выбор и реализация методов и способов защиты информации в информационных системах персональных данных осуществляются на основе Модели угроз и в зависимости от уровня защищенности персональных данных в информационных системах персональных данных.

4.8. Выбранные и реализованные методы и способы защиты персональных данных в информационных системах персональных данных должны обеспечивать нейтрализацию выявленных угроз безопасности персональных данных при их обработке в информационных системах персональных данных в составе системы защиты персональных данных.

4.9. Для проведения работ по выбору и реализации методов и способов защиты персональных данных (включая техническое проектирование системы защиты персональных данных, внедрение средств защиты персональных данных, сопровождение средств защиты персональных данных и т. д.) могут привлекаться подрядные организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

4.10. Общие технические требования по защите персональных данных в информационных системах персональных данных образовательной организации приведены в разделе 5.

5.Обеспечение технической защиты персональных данных

5.1.Общие требования

5.1.1. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных должно осуществляться на всех стадиях жизненного цикла информационных систем персональных данных и состоять из согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности

персональных данных в информационных системах персональных данных, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и нормального функционирования информационных систем персональных данных в случае реализации угроз.

5.1.2. В целях защиты персональных данных от несанкционированного доступа и иных неправомерных действий мероприятия по организации и техническому обеспечению безопасности персональных данных для каждой информационной системы персональных данных должны включать:

а) определение уровней защищенности персональных данных в информационной системе персональных данных на основании Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

б) выявление и закрытие технических каналов утечки персональных данных на основе анализа и актуализации Модели угроз безопасности персональных данных;

в) выбор и реализацию организационных и технических методов и способов защиты информации в информационной системе в зависимости от уровня защищенности персональных данных в информационной системе персональных данных с учетом особенностей инфраструктуры и с учетом актуальных угроз безопасности персональных данных в информационной системе персональных данных;

г) установку, настройку и применение соответствующих программных, аппаратных и программно-аппаратных средств защиты информации;

д) разработку дополнений к трудовым договорам (или должностным инструкциям) по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных для персонала, задействованного в эксплуатации данной информационной системе персональных данных (подразделы А1 и А2 Приложения А).

5.1.3. Предотвращение утечки персональных данных по техническим каналам за счет побочных электромагнитных излучений и наводок, а также за счет электроакустических преобразований реализуется в образовательной организации организационными мерами и не требует специальных технических решений.

5.1.4. Защита персональных данных при их обработке в информационной системе персональных данных от несанкционированного доступа и иных неправомерных действий должна осуществляться в образовательной организации следующими методами и способами:

- реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (включая персональные данные), информационной системе, содержащей персональные данные и связанные с ее работой документами (подраздел Е1 Приложения Е);
- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, содержащие персональные данные;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам (включая персональные данные), программным средствам обработки (передачи) и защиты персональных данных;
- регистрация действий пользователей и обслуживающего персонала информационной системы персональных данных, мониторинг попыток несанкционированного доступа;
- учет и хранение съемных носителей информации с персональными данными и их обращение, исключающее хищение, подмену и уничтожение (подраздел 5.3.ниже);
- использование защищенных каналов связи, используемых для передачи персональных данных;

– размещение технических средств, позволяющих осуществлять обработку персональных данных в пределах контролируемой территории;

– предотвращение внедрения в информационную систему персональных данных вредоносных программ (программ-вирусов) и программных закладок;

– регистрация событий и мониторинг процессов обработки информации;

– контроль целостности программных средств;

– регистрация запуска (остановки) программ обработки персональных данных;

– регистрация вывода персональных данных на печать.

5.1.5. При организации взаимодействия информационной системы персональных данных с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с указанными методами и способами должны применяться следующие дополнительные методы и способы защиты персональных данных от несанкционированного доступа:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы персональных данных;

– защита персональных данных при их передаче по каналам связи;

– использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

– использование средств антивирусной защиты.

5.1.6. Должна производиться периодическая проверка электронных журналов безопасности, в которых регистрируются события безопасности. К электронным журналам безопасности относятся:

– журналы безопасности операционных систем;

– журналы событий системы управления базами данных;

- журналы событий средств защиты информации;
- журналы событий системы контроля и управления физическим доступом;
- журналы событий прикладного программного обеспечения;
- журналы активных сетевых устройств.

5.1.7. К событиям безопасности в информационной системе персональных данных относятся следующие события:

- доступ (входа и выхода в систему и доступа к объектам, в том числе неудачные попытки доступа);
- создание и удаление пользователей;
- изменение прав доступа и привилегий;
- подключение и отключение внешних устройств;
- изменение настроек средств защиты;
- события, генерируемые средствами защиты.

5.1.8. В образовательной организации также могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности персональных данных.

5.1.9. Конкретные методы и средства защиты персональных данных в информационной системе персональных данных должны определяться на основании нормативно-методических документов ФСТЭК России и ФСБ России, исходя из уровней защищенности персональных данных в информационной системе персональных данных и актуальных угроз безопасности персональных данных.

5.1.10. Все технические средства защиты информации должны быть снабжены инструкциями по эксплуатации.

5.1.11. Должен вестись учет технических средств защиты информации, эксплуатационной и технической документации к ним. Форма журнала учета технических средств защиты информации приведена в приложении (подраздел Г1 Приложения Г).

5.1.12. Ответственность за ведение и поддержание в актуальном состоянии журнала учета технических средств защиты информации возлагается на Ответственного за обеспечение безопасности персональных данных.

5.2. Контроль выполнения требований по защите персональных данных

5.2.1. В соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119, должен проводиться периодический контроль выполнения требований по обеспечению безопасности персональных данных (не реже одного раза в три года).

5.2.2. Контроль функций системы защиты производится в рамках мероприятий, описанных в подразделе 7.2 настоящего Положения.

5.2.3. Ответственность за контроль функций системы защиты персональных данных возлагается на ответственного за обеспечение безопасности персональных данных.

5.3. Учет съемных электронных носителей персональных данных

5.3.1. В образовательной организации должен вестись учет защищаемых съемных носителей персональных данных. К защищаемым носителям персональных данных относятся следующие:

- носители информации серверов;
- носители информации автоматизированного рабочего места;
- внешние запоминающие устройства (флеш-накопители, карты памяти и т. п.), содержащие персональные данные.

5.3.2. Форма журнала учета защищаемых съемных электронных носителей приведена в приложении (подраздел Г2 Приложения Г).

5.3.3. Ответственность за учет защищаемых электронных носителей персональных данных возлагается на ответственного за обеспечение безопасности персональных данных.

6. Обязанности персонала

Должностные инструкции ответственного за организацию обработки персональных данных и ответственного за обеспечение безопасности персональных данных расширены с учетом специфики обработки и защиты персональных данных (подразделы А1 и А2 Приложения А). Работники, назначаемые на данные роли, ознакомляются под подпись со своими должностными инструкциями.

6.1. Обязанности ответственного за организацию обработки персональных данных

6.1.1. В обязанности ответственного за организацию обработки персональных данных входит:

- осуществление внутреннего контроля за соблюдением образовательная организациям и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников образовательной организации положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- прием и обработка обращений субъектов персональных данных и их законных представителей (ведение журнала учета обращений субъектов персональных данных, анализ правомерности запросов, составление и отправка ответов);
- прием и обработка запросов уполномоченного органа по защите прав субъектов персональных данных (ведение журнала учета запросов

уполномоченного органа по защите прав субъектов персональных данных, анализ правомерности запросов, составление и отправка ответов);

– ведение и хранение журнала учета проверок уполномоченным органом по защите прав субъектов персональных данных;

– уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных, об изменениях в реквизитах оператора персональных данных;

– уведомление уполномоченного органа по защите прав субъектов персональных данных по запросу этого органа с предоставлением необходимой информации в течение тридцати дней[1] с даты получения такого запроса.

6.1.2. Ответственный за организацию обработки персональных данных обладает следующими полномочиями:

– запрашивать необходимую информацию у руководства и работников образовательной организации, относящуюся к обработке персональных данных и необходимую для выполнения его обязанностей;

– контролировать выполнение обязанностей ответственным за обеспечение безопасности персональных данных, инженерами по телекоммуникации (техниками), а также выполнение требований законодательства и внутренних нормативных документов образовательной организации, регламентирующих обработку и обеспечение безопасности персональных данных;

– назначать ответственного за уничтожение персональных данных и контролировать выполнение процедуры уничтожения персональных данных. Для выполнения уничтожения персональных данных на бумажном носителе в качестве лица, ответственного за уничтожение персональных данных, назначается владелец бизнес-процесса, в случае с другими носителями персональных данных или если обработка персональных данных осуществляется в информационной системе персональных данных, в качестве

[1] Ст. 20 ч. 4 ФЗ «О персональных данных»

лица, ответственного за уничтожение персональных данных, назначается владелец информационной системы персональных данных;

– согласовывать заявки временного или разового допуска работника к работе с персональными данными в связи со служебной необходимостью.

6.2. Обязанности ответственного за обеспечение безопасности персональных данных

6.2.1. В обязанности ответственного за обеспечение безопасности персональных данных входит:

– предоставление и прекращение доступа пользователей к персональным данным в информационных системах персональных данных в соответствии с утвержденным Перечнем должностей работников, допущенных к работе с персональными данными, или с утвержденными заявками на доступ к персональным данным;

– управление учетными записями пользователей комплекса информационных систем персональных данных совместно с инженерами по телекоммуникации (техниками);

– проведение контрольных мероприятий (подраздел 5.2. выше);

– предоставление сведений о персональных данных ответственному за организацию обработки персональных данных в рамках проведения учета защищаемых носителей и проведения инвентаризации (подраздел 5.3. выше);

– установка, конфигурирование и администрирование аппаратных и программных средств защиты информации комплекса информационных систем персональных данных;

– поддержание штатной работы комплекса информационных систем персональных данных совместно с инженерами по телекоммуникации (техниками);

– учет защищаемых носителей персональных данных (подраздел 5.3. выше);

– учет технических средств защиты информации (пункт 5.1.11 подраздела 5.1. выше);

– периодические ежемесячные[2] проверки журналов безопасности (пункт 5.1.6. подраздела 5.1. выше);

– анализ защищенности информационных систем персональных данных;

– организация процесса обучения работников по направлению обеспечения безопасности персональных данных;

– участие в проведении внутреннего контроля и служебных расследований фактов нарушения установленного порядка обработки и обеспечения безопасности персональных данных (подразделы 7.2. и 7.3. ниже).

6.2.2. Ответственный за обеспечение безопасности персональных данных обладает следующими полномочиями:

– проводит плановые и внеплановые контрольные мероприятия в целях контроля, изучения и оценки фактического состояния защищенности персональных данных;

– запрашивает необходимую информацию у очевидцев и подозреваемых лиц при проведении разбирательств по фактам нарушения установленного порядка обработки и обеспечения безопасности персональных данных.

7. Организация внутреннего контроля обработки и обеспечения безопасности персональных данных

7.1. Цели организации внутреннего контроля

7.1.1. Организация внутреннего контроля процесса обработки персональных данных в образовательной организации осуществляется в целях изучения и оценки фактического состояния защищенности персональных данных, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

[2] Периодичность проверки зависит от срока хранения информации в журналах безопасности, например, если информация в журнале безопасности хранится одну неделю, то проверки необходимо проводить еженедельно

7.1.2. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности персональных данных направлены на решение следующих задач:

- обеспечение соблюдения работниками образовательной организации требований настоящего Положения и нормативных правовых актов, регулирующих защиту персональных данных;
- оценка компетентности персонала, задействованного 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.

7.2. Проведение контрольных мероприятий

7.2.1. Контрольные мероприятия (проверки) проводятся на плановой основе, а также при необходимости внепланово.

7.2.2. Решение о необходимости проведения внеплановых контрольных мероприятий принимает ответственный за обеспечение безопасности персональных данных. Данное решение должно быть обосновано возросшими

рисками информационной безопасности для обрабатываемых персональных данных и при существенных изменениях в среде обработки персональных данных.

7.2.3. Контрольные мероприятия (проверки) организуются ответственным за обеспечение безопасности персональных данных.

7.2.4. Плановые проверки проводятся не реже одного раза в полугодие и включают в себя:

- проверку деятельности работников образовательной организации, допущенных к работе с персональными данными в информационных системах персональных данных, на соответствие порядку обработки и обеспечения безопасности персональных данных, установленному Положением по работе с персональными данными и другими нормативными правовыми актами, принятыми в образовательной организации и обязательными для ознакомления и исполнения соответствующими категориями работников;
- проверку работоспособности и эффективности технических средств информационных систем персональных данных и средств защиты персональных данных;
- проверку ведения эталонных копий средств защиты;
- проверку соответствия предоставленных прав доступа пользователей к персональным данным утвержденной матрице доступа;
- проверку минимальной длины и сложности паролей;
- проверку периодичности смены паролей;
- проверку отсутствия на автоматизированных рабочих местах пользователей средств разработки;
- проверку отсутствия на автоматизированных рабочих местах пользователей нештатного программного обеспечения;
- мониторинг журналов протоколирования событий аутентификации.

7.2.5. Ответственный за обеспечение безопасности персональных данных составляет план контрольных мероприятий на полугодие, в котором

определяет состав и периодичность проведения проверок на данный период времени.

7.2.6. Результаты проверок оформляются актами. Выявленные в ходе проверок нарушения, а также отметки об их устранении фиксируются в журнале учета выявленных нарушений в порядке обработки и обеспечения безопасности персональных данных.

7.2.7. Выявленные нарушения расследуются в соответствии с подразделом 7.3.

7.2.8. При необходимости должны быть предложены меры по минимизации последствий выявленных угроз информационной безопасности.

7.2.9. В случае передачи части функций в области информационных технологий сторонним организациям указанные контрольные мероприятия осуществляют эти сторонние организации. Требования по осуществлению контрольных мероприятий указываются в договорах с этими сторонними компаниями.

7.3. Порядок проведения разбирательств

7.3.1. Проведение разбирательств может быть инициировано в одном из следующих случаев:

- обращение субъекта персональных данных по поводу неправомерных действий с его персональными данными;
- выявление нарушений работниками образовательной организации в рамках выполнения своих должностных обязанностей, связанных с обработкой или защитой персональных данных;
- выявление нарушений, приводящих к снижению уровня защищенности персональных данных, в ходе проведения проверок состояния защищенности персональных данных.

7.3.2. В ходе проведения расследования ответственным за обеспечение безопасности персональных данных проводится опрос очевидцев и подозреваемых лиц, предположительно допустивших нарушение.

7.3.3. В ходе проведения опроса выясняется:

– дата и время совершения нарушения;

– обстоятельства, при которых были совершены действия, приведшие к возникновению нарушения;

– последствия, возникшие вследствие совершения нарушения.

7.3.4. Все опрашиваемые лица должны предоставить объяснительные записки (показания, изложенные на бумажном носителе с подписью опрашиваемого).

7.3.5. Ответственный за обеспечение безопасности персональных данных оценивает последствия, возникшие вследствие совершения нарушения.

7.3.6. По результатам разбирательства ответственный за обеспечение безопасности персональных данных в течение трех рабочих дней составляет заключение по результатам разбирательств.

7.3.7. В заключении должны быть приведены:

– краткая справка по нарушению, в отношении которого проводилось разбирательство;

– лицо(а), которое совершило(и) нарушение;

– предложения по привлечению виновника к юридической ответственности (дисциплинарной ответственности: замечание, выговор, увольнение; или к гражданско-правовой ответственности (взыскание причиненного ущерба) и/или применении к нему мер дисциплинарного воздействия (депремирование, указание на недостатки и т. п.);

– план мероприятий по предотвращению подобных нарушений в будущем (если уместно).

7.3.8. Заключение предоставляется ответственному за организацию обработки персональных данных и согласовывается с директором образовательной организации.

7.3.9. Срок проведения расследования не должен превышать семи рабочих дней.