

## Инструкция администратора безопасности информации

### 1. Общие положения

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и определяет порядок обеспечения безопасности информации при проведении работ администратором безопасности информации (далее – АБИ) в информационных системах (далее – информационная система; ИС) МБОУ СОШ №14 (далее – Организация).

1.2. Субъектами доступа к ресурсам ИС являются пользователи, АБИ и обслуживающий персонал (работники, осуществляющие техническое обслуживание, ремонт), в соответствии с утвержденным перечнем.

1.3. Обрабатываемая в ИС информация содержит сведения, составляющие персональные данные.

1.4. АБИ назначается приказом руководителя Организации и получает неограниченные права на доступ к ресурсам ИС.

1.5. АБИ осуществляет общее руководство и контроль за обеспечением безопасности информации при работе пользователей ИС и обслуживающего персонала.

1.6. Методическое руководство по информационной безопасности объектов информатизации осуществляет АБИ.

1.7. АБИ имеет право вносить предложения по изменению и дополнению данной Инструкции, а также «Инструкции пользователя».

1.8. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

### 2. Термины и определения

2.1. **Администратор безопасности информации** – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системой защиты информации в соответствии с установленной ролью.

2.2. **Безопасность информации [данных]** – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

2.3. **Доступность информации [ресурсов информационной системы]** – состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

2.4. **Защищаемая информация** – информация, для которой обладателем информации определены характеристики ее безопасности.

2.5. **Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

2.6. **Информация** – сведения (сообщения, данные) независимо от формы их представления.

2.7. **Конфиденциальность информации** – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

2.8. **Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

2.9. **Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

2.10. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.11. **Пользователь** – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

2.12. **Средство защиты информации** – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.

2.13. **Техническое средство** – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

### 3. Требования к администратору безопасности информации

3.1. АБИ обязан знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

3.2. АБИ, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами ИС не допускается.



**3.3.** АБИ осуществляет учет съемных машинных носителей информации, их уничтожение, либо контроль процедуры их уничтожения.

**3.4.** АБИ обязан немедленно реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем (далее – ОТСС и ВТСС), СЗИ, системного и прикладного программного обеспечения (далее – ПО) ИС.

**3.5.** АБИ обязан немедленно ставить в известность ответственного за организацию обработки и обеспечение безопасности персональных данных (ответственного за защиту информации) Организации обо всех неисправностях аппаратно-программных средств ИС.

**3.6.** АБИ обязан ставить в известность ответственного за защиту информации Организации о необходимости проведения работ по администрированию СЗИ.

**3.7.** АБИ имеет право проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки персональных данных.

**3.8.** АБИ разрабатывает планы мероприятий по администрированию и техническому обслуживанию аппаратных и программных средств ИС Организации.

**3.9.** АБИ обязан в случае отказа технических средств или программного обеспечения элементов ИС, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

**3.10.** АБИ имеет право требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИС или средств защиты.

**3.11.** АБИ присутствует при выполнении технического обслуживания элементов ИС сторонними специалистами на территории Организации.

**3.12.** АБИ осуществляет разбирательства и составление заключений по фактам несоблюдения условий хранения носителей информации, нарушения правил работы с техническими и программными средствами ИС, в том числе с СЗИ, или по другим нарушениям, которые могут привести к снижению уровня информационной безопасности.

**3.13.** В ходе управления (администрирования) системой защиты информации АБИ обязан осуществлять:

- заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИС;
- управление СЗИ в ИС, в том числе параметрами настройки программного обеспечения, включая программное обеспечение СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;
- изменение аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении системы защиты информации ИС;
- установку обновлений программного обеспечения, включая программное обеспечение СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;
- централизованное управление системой защиты информации ИС (при необходимости);
- регистрацию и анализ событий в ИС, связанных с защитой информации;
- информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИС и отдельных СЗИ, а также их обучение;
- сопровождение функционирования системы защиты информации ИС в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

**3.14.** В ходе выявления инцидентов и реагирования на них АБИ обязан осуществлять:

- обнаружение и идентификацию инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;



- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

**3.15.** В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС, АБИ обязан осуществлять:

- анализ и оценку функционирования СЗИ, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИС;
- проверку работоспособности и параметров настройки программного обеспечения, аппаратных и программных СЗИ;
- проверку состава технических средств, программного обеспечения и СЗИ;
- контроль целостности печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных;
- еженедельное отслеживание появления новых видов уязвимостей ПО ИС. По необходимости АБИ производит устранение уязвимостей согласно рекомендациям разработчика;
- периодический анализ изменения угроз безопасности информации в ИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;
- контроль за событиями безопасности и действиями пользователей в ИС. В частности, АБИ обязан осуществлять постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации;
- контроль (анализ) защищенности информации, содержащейся в ИС;
- документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС;
- принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИС, повторной аттестации ИС или проведении дополнительных аттестационных испытаний.

#### **4. Доступ к ресурсам информационной системы**

**4.1.** Обязательными условиями получения доступа к ресурсам ИС АБИ являются:

- право доступа в помещение;
- наличие допуска к защищаемой информации;
- право доступа к ИС;
- знание технологии обработки информации в ИС с учетом требований информационной безопасности.

**4.2.** Идентификация АБИ в ИС осуществляется по уникальному имени и персональному идентификатору (при его наличии).

**4.3.** Длина пароля АБИ и всех пользователей – не менее 6 буквенно-цифровых символов.



**4.4.** Уникальное имя, персональный идентификатор (при его наличии) и пароль АБИ получает в установленном порядке. АБИ обязан их помнить и не допускать раскрытия, не допускается запись на каких-либо носителях в целях напоминания. Во время ввода пароля на клавиатуре должна быть исключена возможность его просмотра другими лицами. Не допускается оставление без присмотра и передача другим лицам персонального идентификатора (при его наличии).

**4.5.** При утере или подозрении на утечку своего имени, пароля или персонального идентификатора АБИ должен немедленно изменить свои идентификационные данные и проконтролировать возможные изменения в настройках СЗИ.

**4.6.** Регистрация пользователя осуществляется АБИ в соответствии с «Инструкцией по организации парольной защиты» и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора (при его наличии) и назначении пароля.

**4.7.** При заведении новой учетной записи, АБИ должен проверить личность пользователя и его должностные обязанности.

**4.8.** Предоставление пользователям прав доступа к объектам доступа ИС должно осуществляться на основании задач, решаемых пользователями.

**4.9.** АБИ не имеет права требовать у пользователей раскрытия их паролей, а также передачи ему персональных идентификаторов (при их наличии), кроме случая изменения идентификационных данных.

**4.10.** АБИ имеет право требовать у пользователя изменения его пароля, но не имеет права самостоятельно изменять его пароль.

## **5. Порядок работы администратора безопасности информации с ресурсами информационной системы**

Ниже приводится перечень работ, производимых АБИ с ресурсами ИС.

### **5.1. Проверка работоспособности и настройка системы доступа к ресурсам ИС**

АБИ присваивает пользователям идентификационные данные к ресурсам ИС. При этом должны выполняться следующие требования:

- АБИ определяет политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;
- АБИ сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, далее кодирует персональный идентификатор (при его наличии) пользователя;
- изменение учетных данных пользователя производится АБИ по требованию ответственного за защиту информации Организации, а также периодически по утвержденному плану и в случае увольнения работника;
- АБИ имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, если попытка взлома была успешной, АБИ обязан потребовать у пользователя изменение пароля.

### **5.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации (СЗИ)**

АБИ обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – работы прекратить.

В случае сбоя СЗИ, таких, как неправильная идентификация пользователей, АБИ обязан приостановить обработку информации до устранения неисправности. В случае производственной необходимости – отключить СЗИ и лично контролировать проведение работ пользователями.

### **5.3. Антивирусная защита ресурсов ИС**



АБИ разрабатывает и контролирует реализацию антивирусной политики, а именно:

- настраивает параметры антивирусной программы;
- контролирует работоспособность антивирусной программы;
- немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы и принимает соответствующие меры;
- имеет право на проведение внеплановой проверки на наличие вирусов;
- периодически (один раз в неделю) контролирует корректность процесса обновления антивирусных баз, а также исполняемых модулей антивирусной программы.

#### **5.4. Хранение дистрибутивов программного обеспечения СЗИ**

АБИ должен хранить дистрибутивы программного обеспечения СЗИ и прикладного программного обеспечения, установленного в ИС Организации в месте, исключающем доступ посторонних лиц.

#### **5.5. Проверка целостности системного и прикладного ПО**

Контролю целостности подлежат файлы ПО ИС с расширениями: \*.exe, \*.com, \*.dll, \*.sys, \*.vxd, \*.drv.

#### **5.6. Резервное копирование и восстановление информации**

Резервное копирование производится регулярно с заданной периодичностью, а также в случае производственной необходимости. При этом необходимо выполнять следующие требования:

- обязательное резервное копирование производится в случае обнаружения неисправностей в работе ПЭВМ или отчуждаемых машинных носителей (далее – МН);
- допускается обоснованное внеплановое резервное копирование информации как по инициативе пользователя, так и АБИ, если это не нарушает технологию обработки информации;
- резервные копии пользовательской информации и информации операционной системы хранятся на учетных внешних МН;
- ответственным лицом за хранение резервных копий является АБИ.

По мере устранения неисправностей ПЭВМ АБИ производит восстановление информации ограниченного доступа с резервных копий.

АБИ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИС в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

#### **5.7. Конфигурирование ИС**

Конфигурационной единицей являются услуги, оборудование, программное обеспечение, здания, люди, документы и пр.

Управление изменениями конфигурации осуществляет ответственный за защиту информации. Планирование реализации и непосредственно реализация необходимых изменений возлагается на АБИ.

В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации АБИ обязан осуществлять:

- поддержание конфигурации ИС и ее системы защиты информации (структуры системы защиты информации ИС, состава, мест установки и параметров настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИС и ее системы защиты информации);



- управление изменениями базовой конфигурации ИС и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИС и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИС и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИС и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации;
- анализ потенциального воздействия планируемых изменений в базовой конфигурации ИС и ее СЗИ на обеспечение информационной безопасности, возникновение дополнительных угроз безопасности информации и работоспособность ИС;
- определение параметров настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС и ее системы защиты информации;
- внесение информации (данных) об изменениях в базовой конфигурации ИС и ее системы защиты информации в документацию на СЗИ;
- принятие решения по результатам управления конфигурацией о повторной аттестации ИС или проведении дополнительных аттестационных испытаний.

Обязанности по управлению изменениями в аппаратном и программном обеспечении и всех элементах документации, которые связаны с работой, поддержкой и сопровождением систем, находящихся в эксплуатации, возлагаются на АБИ. При возникновении необходимости изменения конфигурации ИС, аттестованной по требованиям безопасности информации, АБИ согласовывает планируемые изменения с предприятием-лицензиатом, проводившим аттестационные испытания.

#### **5.8. Вывод ресурсов ИС из эксплуатации**

При невозможности ремонта различных ресурсов ИС АБИ обязан:

- физически уничтожать любые МН, независимо от содержащейся на них информации; картриджи принтера, иные комплектующие могут быть использованы за пределами ИС;
- факт выхода из строя и замены оборудования должен быть отражен в Техническом паспорте на ИС.

#### **5.9. Реагирование на сбои при регистрации событий безопасности**

Реагирование на сбои при регистрации событий безопасности осуществляется АБИ путем изменения параметров сбора, записи и хранения информации о событиях безопасности в журналах СЗИ от НСД, в том числе отключение записи информации о событиях безопасности от части компонентов ИС, запись поверх устаревших хранимых записей событий безопасности.

В случае выявления признаков инцидентов безопасности, АБИ обязан:

- немедленно уведомить руководителя о данном факте;
- по возможности в максимально сжатые сроки установить причину возникновения инцидента и исключить возможность его повторения;
- восстановить работоспособность ИС;
- по окончании работ по восстановлению работоспособности ИС произвести запись в соответствующих журналах.

### **6. Действия при обнаружении попыток несанкционированного доступа**



**6.1.** К попыткам несанкционированного доступа относятся:

- сеансы работы с ИС незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;
- действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИС, при использовании учетной записи администратора или другого пользователя ИС, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

**6.2.** При выявлении факта несанкционированного доступа АБИ обязан:

- пресечь дальнейший несанкционированный доступ к ИС;
- доложить ответственному за защиту информации Организации служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;
- известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

## **7. Ответственность**

**7.1.** АБИ несет персональную ответственность за:

- сохранность носителей информации и содержащейся на них информации в рабочее время;
- несоблюдение требований данной Инструкции и неправомерное использование ресурсов ИС;
- СЗИ, применяемые в ИС Организации;
- качество проводимых работ по обеспечению безопасности информации и за все действия, совершенные от имени учетной записи АБИ в ИС, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования учетной записи.

**7.2.** АБИ при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

