

**УТВЕРЖДАЮ**

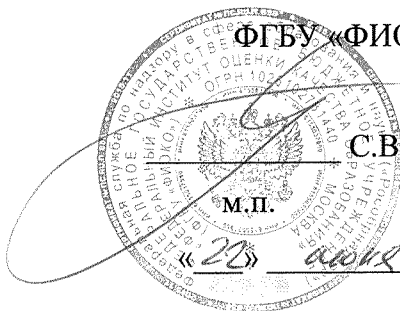
Директор

**ФГБУ «ФИОКО»**

С.В. Станченко

М.П.

«22» \_\_\_\_\_ 2018 г.



**ПОЛОЖЕНИЕ**

**об обеспечении безопасности конфиденциальной информации в Федеральном  
государственном бюджетном учреждении «Федеральный институт оценки качества  
образования»**

## СОДЕРЖАНИЕ

<b>1 ОБЩИЕ ПОЛОЖЕНИЯ .....</b>	<b>Ошибка! Закладка не определена.</b>
<b>2 ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ.....</b>	<b>Ошибка! Закладка не определена.</b>
2.1 Система защиты конфиденциальной информации .....	4
2.2 Назначение ответственных лиц .....	4
2.3 Пользователи информационных систем .....	5
<b>3 СРЕДСТВА И МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ .....</b>	<b>6</b>
3.1 Применяемые средства защиты информации .....	6
3.2 Организационные меры .....	6
3.3 Технические меры .....	7
3.4 Контроль применяемых мер защиты.....	7
<b>4 ОРГАНИЗАЦИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ.....</b>	<b>9</b>
<b>5 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ .....</b>	<b>10</b>
Приложение 1 .....	11
Приложение 2 .....	13
Приложение 3 .....	14

## **1 Введение**

Положение об обеспечении безопасности конфиденциальной информации при ее обработке в информационных системах Федерального государственного бюджетного учреждения «Федеральный институт оценки качества образования» (далее – Положение) разработано в соответствии с Конституцией Российской Федерации (далее – РФ), Федеральным законом от 30.12.2001 «Трудовым кодексом Российской Федерации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Настоящее Положение определяет порядок организации работ, а также средства и меры по обеспечению безопасности конфиденциальной информации при их обработке в информационных (далее – ИС) Федерального государственного бюджетного учреждения «Федеральный институт оценки качества образования» (далее – ФГБУ «ФИОКО»).

Действие Положения распространяется на все структурные подразделения ФГБУ «ФИОКО».

Настоящее Положение доводится до сведения всех работников ФГБУ «ФИОКО» в части, касающейся обработки конфиденциальной информации, в том числе персональных данных, а также в полном объеме до работников, осуществляющих обработку конфиденциальной информации, под роспись.

Все изменения в настоящее Положение вносятся приказом Директора ФГБУ «ФИОКО».

## **2 Организация работ по обеспечению безопасности конфиденциальной информации**

### **2.1 Система защиты конфиденциальной информации**

Безопасность конфиденциальной информации при ее обработке в ИС обеспечивается с помощью системы защиты, включающей организационные и технические меры по защите конфиденциальной информации. Выбор и реализация методов и способов защиты конфиденциальной информации в ИС осуществляется на основании уровня защищенности конфиденциальной информации при ее обработке в ИС, исходя из угроз безопасности конфиденциальной информации.

Система защиты конфиденциальной информации ФГБУ «ФИОКО» должна обеспечивать:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа (далее – НСД) к конфиденциальной информации и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСД к конфиденциальной информации;
- недопущение воздействия на технические средства автоматизированной обработки конфиденциальной информации, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления конфиденциальной информации, модифицированной или уничтоженной вследствие НСД к ней;
- постоянный контроль обеспечения уровня защищенности конфиденциальной информации.

Разработка и проведение мероприятий по обеспечению безопасности конфиденциальной информации при ее обработке в ИС, осуществляется силами и средствами ФГБУ «ФИОКО» либо сторонними организациями на договорной основе, имеющими лицензию на право проведения работ по технической защите конфиденциальной информации.

### **2.2 Назначение ответственных лиц**

Лицо ответственное за обеспечение безопасности конфиденциальной информации в ФГБУ «ФИОКО» назначается и освобождается от обязанностей приказом Директора.

Лицо ответственное за обеспечение безопасности конфиденциальной информации подчиняется непосредственно Директору и подотчетно ему.

Лицо ответственное за обеспечение безопасности конфиденциальной информации

обязано:

- осуществлять координацию организационных мероприятий, направленных на обеспечение защиты конфиденциальной информации при ее обработке в информационных системах;
- обеспечивать доведение до работников ФГБУ «ФИОКО» положений законодательства РФ о требованиях к защите конфиденциальной информации;
- участвовать в планирование мероприятий по защите информации и осуществлению контроля их выполнения и эффективности;
- осуществлять внутренний контроль за соблюдением в ФГБУ «ФИОКО» законодательства РФ о защите конфиденциальной информации.

### 2.3 Пользователи информационных систем

Работники, доступ которых к конфиденциальной информации, обрабатываемым в ИС, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим конфиденциальной информации на основании Перечня должностей, утверждаемого Директором ФГБУ «ФИОКО». Соответствие лиц и занимаемых ими должностей приведено в штатном расписании. При обработке конфиденциальной информации в ИС вышеуказанные лица должны соблюдать требования внутренних документов ФГБУ «ФИОКО» по обеспечению безопасности информации.

### **3 Средства и меры по обеспечению безопасности конфиденциальной информации при их обработке в информационных системах**

Компания при обработке конфиденциальной информации принимает необходимые правовые, организационные и технические меры для защиты конфиденциальной информации от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения конфиденциальной информации, а также от иных неправомерных действий в отношении конфиденциальной информации.

#### **3.1 Применяемые средства защиты информации**

Средства защиты информации (далее – СЗИ), применяемые в информационных системах ФГБУ «ФИОКО», в установленном законодательством РФ порядке, проходят процедуру оценки соответствия.

СЗИ, предназначенные для обеспечения безопасности конфиденциальной информации при их обработке в информационных системах, а также эксплуатационная и техническая документация к ним подлежат учету в соответствии с порядком, определенным в ФГБУ «ФИОКО».

До ввода в эксплуатацию все средства защиты конфиденциальной информации, устанавливаемые в ФГБУ «ФИОКО», проходят проверку готовности их использования с составлением заключения о возможности их эксплуатации (форма заключения приведена в Приложении 1 к настоящему Положению). При положительном заключении о возможности эксплуатации данные средства вводятся в эксплуатацию с составлением акта (форма акта внедрения средств защиты информации приведена в Приложении 2 к настоящему Положению). Проверка и ввод средств защиты производится комиссией, назначенной приказом Директора ФГБУ «ФИОКО».

Установка и ввод таких средств в эксплуатацию осуществляется в соответствии с эксплуатационной и технической документацией на СЗИ.

Контроль соблюдения порядка и условий использования СЗИ, предусмотренных эксплуатационной и технической документацией, возлагается на Лицо ответственное за обеспечение безопасности конфиденциальной информации.

Работники ФГБУ «ФИОКО», использующие СЗИ, применяемые в ИС, должны быть обучены правилам работы с ними.

#### **3.2 Организационные меры**

Для обеспечения безопасности конфиденциальной информации при их обработке в

ИС ФГБУ «ФИОКО» применяются следующие организационные меры:

- обеспечение учета, хранения, обращения и уничтожения носителей конфиденциальной информации;
- ознакомление работников с внутренними требованиями ФГБУ «ФИОКО» по защите конфиденциальной информации;
- обеспечение контроля доступа в помещения, в которых находятся технические средства обработки конфиденциальной информации, хранятся носители конфиденциальной информации;
- размещение технических средств обработки конфиденциальной информации в пределах контролируемой зоны;
- обеспечение пропускного режима на территорию ФГБУ «ФИОКО», охраны помещений с установленными техническими средствами обработки конфиденциальной информации.

### **3.3 Технические меры**

Для обеспечения безопасности конфиденциальной информации при их обработке в ИС ФГБУ «ФИОКО» применяются следующие технические меры:

- установление и реализация правил предоставления доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты конфиденциальной информации;
- регистрация и учет действий пользователей, совершаемых с конфиденциальной информацией в ИС;
- применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности конфиденциальной информации;
- осуществление антивирусного контроля;
- обеспечение восстановления конфиденциальной информации, модифицированной или уничтоженной вследствие НСД к ней;
- применение средств межсетевое экранирования;
- централизованное управление системой защиты конфиденциальной информации.

### **3.4 Контроль применяемых мер защиты**

С целью поддержания уровня защищенности конфиденциальной информации в ФГБУ «ФИОКО» реализована система контроля применяемых мер по защите конфиденциальной информации.

В ходе мероприятий по контролю осуществляется:

- проверка выполнения требований нормативных документов по защите конфиденциальной информации;
- оценка обоснованности и эффективности принимаемых мер по обеспечению безопасности конфиденциальной информации до ввода в эксплуатацию ИС;
- систематическое проведение мониторинга действий пользователей, доведение его результатов до сведения руководства ФГБУ «ФИОКО», проведение разбирательств и составление заключений по фактам нарушения требований безопасности конфиденциальной информации (форма заключения приведена в Приложении 4 к настоящему Положению).

Перечень мероприятий по контролю, его периодичность, а также ответственные лица устанавливаются Планом проведения контроля обеспечения безопасности конфиденциальной информации ФГБУ «ФИОКО».

Внутренний контроль принимаемых в ФГБУ «ФИОКО» мер по обеспечению безопасности конфиденциальной информации при их обработке в ИС организует и осуществляет Лицо ответственное за обеспечение безопасности конфиденциальной информации.

Для проведения внешнего контроля и аудита безопасности конфиденциальной информации Компанией на договорной основе может привлекаться сторонняя организация, обладающая лицензией на деятельность по технической защите конфиденциальной информации.



#### **4 ОРГАНИЗАЦИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ**

В целях обеспечения непрерывности деятельности и (или) восстановления функционирования ИС в ФГБУ «ФИОКО» применяется система резервного копирования и восстановления данных.

Практическое решение задач, связанных с резервированием и восстановлением конфиденциальной информации, возлагается на администраторов ИС и администратора безопасности.

Для реализации функции восстановления баз данных осуществляется периодическое резервное копирование информации на внешние машинные носители информации.

Восстановление информации производится в случае ее частичной или полной утраты путем переноса данных с резервных копий на основные носители в соответствии с эксплуатационной документацией на используемую систему восстановления данных. По завершению восстановления осуществляется проверка работоспособности и целостности данных.

В случае применения системы «горячего резервирования» дальнейшая работа может производиться на дублирующем оборудовании. В этом случае данное оборудование переводится в разряд основного, а восстановленная система выполняет функции «горячего резерва».

При нарушении целостности (полной утрате) системного и (или) прикладного программного обеспечения его восстановление производится с исходных дистрибутивов.

По всем случаям утраты конфиденциальной информации проводится анализ причин инцидента с составлением заключения в свободной форме. При этом первичная диагностика выполняется до начала процесса устранения, а по его завершению проводится полная диагностика ИС.

## 5 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Иные права и обязанности работников, допущенных к обработке конфиденциальной информации с использованием средств автоматизации, определяются также их должностными инструкциями.

Лица, виновные в нарушении норм, регулирующих обработку и защиту конфиденциальной информации, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном действующим законодательством.

**Приложение 1**

к Положению об обеспечении безопасности конфиденциальной информации при ее обработке в информационных системах в ФГБУ «ФИОКО»

**ЗАКЛЮЧЕНИЕ № \_\_\_\_\_  
о возможности эксплуатации средства защиты информации**

\_\_\_\_\_ (наименование)

В соответствии с Постановлением Правительства Российской Федерации от 10.11.2012 № 1119 «Об утверждении требований к защите конфиденциальной информации при их обработке в информационных системах» комиссией, назначенной приказом Директора ФГБУ «ФИОКО» от \_\_\_\_\_.\_\_\_\_ № \_\_\_\_\_ «Об организации работ по обработке конфиденциальной информации», в составе:

Председатель комиссии:

\_\_\_\_\_ (должность, фамилия, имя, отчество)

Члены комиссии:

\_\_\_\_\_  
\_\_\_\_\_ (должность, фамилия, имя, отчество)

проведена установка, настройка и проверка готовности

\_\_\_\_\_ (наименование средства защиты информации)

Прикладное программное обеспечение

\_\_\_\_\_ (наименование программного обеспечения, место установки)

Информация о настройках средств защиты информации

\_\_\_\_\_ (наименование документа, по которому проводилась настройка средства защиты информации)

Выполнение требований по сертификации средства защиты информации

---

---

---

---

---

(реквизиты сертификата на средство защиты информации/не проводилась)

**Вывод о возможности эксплуатации: установленное средство защиты информации**

\_\_\_\_\_ (наименование)  
ГОТОВО К ИСПОЛЬЗОВАНИЮ В ИНФОРМАЦИОННОЙ СИСТЕМЕ  
« \_\_\_\_\_ »  
(название ИС)  
в качестве \_\_\_\_\_  
\_\_\_\_\_ (назначение средства защиты информации)

Председатель комиссии

\_\_\_\_\_ (личная подпись) \_\_\_\_\_ (фамилия, имя, отчество)

Члены комиссии

\_\_\_\_\_ (личная подпись) \_\_\_\_\_ (фамилия, имя, отчество)

\_\_\_\_\_ (личная подпись) \_\_\_\_\_ (фамилия, имя, отчество)

\_\_\_\_\_ (личная подпись) \_\_\_\_\_ (фамилия, имя, отчество)

**Приложение 2**

к Положению об обеспечении безопасности конфиденциальной информации при ее обработке в информационных системах в ФГБУ «ФИОКО»

**АКТ № \_\_\_\_\_  
внедрения средств защиты информации**

Комиссия, назначенная приказом Директора ФГБУ «ФИОКО» от \_\_\_\_\_.\_\_\_\_ № \_\_\_\_\_ «Об организации работ по обработке конфиденциальной информации», в составе:

Председатель комиссии:

\_\_\_\_\_ (должность, фамилия, имя, отчество)

Члены комиссии:

\_\_\_\_\_  
\_\_\_\_\_ (должность, фамилия, имя, отчество)

на основании Заключения № \_\_\_\_\_ от \_\_.\_\_.201\_ «О возможности эксплуатации средства защиты информации» составила настоящий акт о том, что средство защиты информации

\_\_\_\_\_ (наименование средства защиты информации)

информационной системы конфиденциальной информации

« \_\_\_\_\_ », (название ИС)

установленное в соответствии с эксплуатационной и технической документацией к нему, вводится в эксплуатацию.

Председатель комиссии

\_\_\_\_\_ (личная подпись)

\_\_\_\_\_ (фамилия, имя, отчество)

Члены комиссии

\_\_\_\_\_ (личная подпись)

\_\_\_\_\_ (фамилия, имя, отчество)

\_\_\_\_\_ (личная подпись)

\_\_\_\_\_ (фамилия, имя, отчество)

**Приложение 3**

к Положению об обеспечении безопасности конфиденциальной информации при ее обработке в информационных системах в ФГБУ «ФИОКО»

**ЗАКЛЮЧЕНИЕ № \_\_\_\_\_  
по факту несоблюдения требований безопасности конфиденциальной информации  
(условий хранения носителей, использования средств защиты информации)**

Комиссия, назначенная приказом Директора ФГБУ «ФИОКО» от \_\_\_\_\_.\_\_\_\_.\_\_\_\_ № \_\_\_\_\_ «Об организации работ по обработке конфиденциальной информации», в составе:

Председатель комиссии:

\_\_\_\_\_

(должность, фамилия, имя, отчество)

Члены комиссии:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(должность, фамилия, имя, отчество)

составила настоящее заключение по факту несоблюдения условий хранения носителей конфиденциальной информации (использования средств защиты информации) работником

\_\_\_\_\_

(наименование структурного подразделения, фамилия, имя и отчество)

Комиссией установлено, что

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

(описание инцидента нарушения безопасности конфиденциальной информации)

**Вывод:** комиссия считает, что вышеперечисленные нарушения стали следствием

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

---

(причины нарушения, предложения о привлечении виновного к ответственности)

Председатель комиссии

\_\_\_\_\_  
(личная подпись)

\_\_\_\_\_  
(фамилия, имя, отчество)

Члены комиссии

\_\_\_\_\_  
(личная подпись)

\_\_\_\_\_  
(фамилия, имя, отчество)

\_\_\_\_\_  
(личная подпись)

\_\_\_\_\_  
(фамилия, имя, отчество)

\_\_\_\_\_  
(личная подпись)

\_\_\_\_\_  
(фамилия, имя, отчество)

### ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	Должность	Фамилия и инициалы	Дата	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				