**Краевое государственное общеобразовательное бюджетное учреждение**
**«Владивостокская специальная (коррекционная) начальная школа–детский сад IV вида»**
**(КГОБУ Владивостокская КШ IV вида )**

690092 Приморский край, г. Владивосток, ул. Волкова, д.3а
тел. 8(423) 228-78-20; 8(423) 225-86-61. E-mail: shkola-sadN3@yandex.ru
ИНН/КПП 2537041510/253701001 ОГРН 1022501804995

УТВЕРЖДЕНО

приказом директора КГОБУ
Владивостокская КШ IV вида

от « 20 » декабря 2024 г.№ 107

_____ Е.Б.Никифорова

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Подписан: Никифорова Елена Борисовна
DN: C=RU, S=Приморский край, L=Владивосток, T=Директор, O="КРАЕВОЕ ГОСУДАРСТВЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ""ВЛАДИВОСТОКСКАЯ СПЕЦИАЛЬНАЯ (КОРРЕКЦИОННАЯ) НАЧАЛЬНАЯ ШКОЛА - ДЕТСКИЙ САД IV ВИДА""", СНИЛС=04190427028, ИНН=253603352767, E=shkola-sadn3@yandex.ru, G=Елена Борисовна, SN=Никифорова, CN=Никифорова Елена Борисовна
Основание: Я являюсь автором этого документа
Дата: 2025.04.14 12:37:11+10'00'

# ПОЛОЖЕНИЕ О ПОРЯДКЕ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В КГОБУ ВЛАДИВОСТОКСКАЯ КШ IV ВИДА

2024 год

**Содержание**

## Перечень терминов и сокращений

| Обозначение | Описание |
|---|---|
| Безопасность информации | состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность. |
| Доступность информации | состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно. |
| Конфиденциальность информации | обязательное для выполнения лицом, получившим доступ к информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. |
| Компьютерный инцидент | факт нарушения и (или) прекращения функционирования «ИС», сети электросвязи, используемой для организации взаимодействия объекта, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки. |
| Межсетевое взаимодействие | Способ соединения компьютерной сети с другими сетями с помощью шлюзов, которые обеспечивают общепринятый порядок маршрутизации пакетов информации между сетями. |
| Несанкционированный доступ (НСД) | доступ к информации или действия с информацией, нарушающие правила разграничения доступа, с использованием штатных средств. |
| Обработка ПДн | любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн. |
| Ответственный за организацию обработки ПДн | лицо, осуществляющее внутренний контроль за соблюдением организацией и его работниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн. |
| Персональные данные (ПДн) | любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн). |
| Средства защиты информации (СЗИ) | техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации. |
| Средства криптографической защиты информации (СКЗИ) | средства шифрования — аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;<br>средства имитозащиты — аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания |

| | |
|---|---|
| | ложной информации;<br>средства электронной подписи (ЭП) — аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание ЭП, подтверждение подлинности ЭП, создание Ключей ЭП. |
| Уполномоченный орган по защите прав субъектов ПДн | федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки ПДн требованиям законодательства Российской Федерации в области ПДн. |
| ФЗ «О персональных данных» | Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных». |

## 1. Общие положения

Целью настоящего положения по организации и проведению работ по обеспечению безопасности персональных данных (далее – ПДн) в КГОБУ Владивостокская КШ IV вида является обеспечение защиты прав субъектов ПДн, а также определение основных целей и задач по обеспечению безопасности информации, структуры системы обеспечения безопасности информации и мер по обеспечению безопасности информации в *КГОБУ Владивостокская КШ IV вида .*

Правила разработаны в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее — Постановление № 1119), Приказом ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», внутренними организационно-распорядительными документами *КГОБУ Владивостокская КШ IV вида* по обеспечению безопасности информации.

Требования настоящих правил обязательны для всех работников, осуществляющих обработку ПДн.

## 2. Цели и задачи обеспечения безопасности информации ***КГОБУ Владивостокская КШ IV вида***

Целью обеспечения безопасности информации является *обеспечение устойчивого функционирования информационной системы персональных данных при проведении в отношении нее компьютерных атак.*

Основными задачами обеспечения безопасности информации являются:

– предотвращение неправомерного доступа к защищаемой информации, обрабатываемой в КГОБУ Владивостокская КШ IV вида_, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

– недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование

– восстановление функционирования компонентов *«информационной системы»*, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации.

## 3. Порядок определения уровня защищенности персональных данных

Определение уровня защищенности осуществляется комиссией, назначенной Приказом директора КГОБУ Владивостокская КШ IV вида__, на основании Постановления № 1119 и в соответствии с порядком, представленным ниже.

Определение уровня защищенности осуществляется комиссией на основании следующей информации:

– актуальная категория угроз;

– тип ИСПДн;

– количество субъектов, чьи ПДн обрабатываются;

– являются ли Субъекты ПДн работниками Учреждения или нет.

В соответствии с п. 5 Постановления № 1119 выделяются следующие типы информационных систем:

**ИСПДн-С**: информационная система, обрабатывающая специальные категории ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн;

**ИСПДн-Б**: информационная система, обрабатывающая биометрические ПДн, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн, и не обрабатываются сведения, относящиеся к специальным категориям ПДн;

**ИСПДн-Д**: информационная система, обрабатывающая общедоступные ПДн субъектов ПДн, полученные только из общедоступных источников ПДн, созданных в соответствии со ст. 8 ФЗ «О персональных данных»;

**ИСПДн-И**: информационная система, обрабатывающая иные ПДн, которые не могут быть отнесены к специальным категориям ПДн, к биометрическим и общедоступным ПДн.

В соответствии с п. 6 Постановления № 1119 под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного доступа к персональным данным при их обработке, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия. Выделяют следующие категории угроз:

– угрозы 1-го типа — угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в «СУИТ»;

– угрозы 2-го типа — угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в «СУИТ»;

– угрозы 3-го типа — угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в «СУИТ».

Для определения уровня защищенности выполняются следующие действия:

– составляется список компонентов, в которых обрабатываются ПДн;

– определяются цели обработки ПДн;

– определяются компоненты, для которых цели обработки ПДн определяют другие юридические лица или государственные органы, и/или Учреждение не является владельцем системы (не является владельцем средств обработки информации), и/или в которых обрабатываются ПДн, не позволяющие определить Субъекта ПДн. Выявленные компоненты исключаются из дальнейшего рассмотрения;

– определяются типы компонентов;

– определяются категории актуальных угроз;

– определяется количество Субъектов ПДн, являющихся работниками Учреждения и не являющихся таковыми;

– определяются уровни защищенности компонентов в соответствии с Постановлением № 1119.

Комиссия фиксирует результаты определения уровня защищенности в «Акте определения уровня защищенности персональных данных». Пересмотр уровня защищенности осуществляется в рамках ежегодного в рамках аудита.

## 4. Уведомление об обработке ПДн

КГОБУ Владивостокская КШ IV вида__ в соответствии со ст. 22 ФЗ «О персональных данных» обязано подать уведомление об обработке ПДн (далее — Уведомление) в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор).

Подготовку, контроль отправки Уведомления в Роскомнадзор, внесение изменений в уведомление в случае необходимости, взаимодействие с Роскомнадзором по вопросам, касающимся уведомления, осуществляет ответственный за организацию обработки ПДн.

Для подготовки уведомления ответственный за организацию обработки ПДн руководствуется требованиями ФЗ «О персональных данных», а также методическими рекомендациями по заполнению Уведомления, размещенными на официальном сайте Роскомнадзора: https://rkn.gov.ru/.

В случае изменения сведений, указанных в уведомлении, а также в случае прекращения обработки ПДн ответственный за организацию обработки ПДн обязан уведомить об этом Роскомнадзор в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки ПДн, посредством отправки информационного письма о внесении изменений в сведения в реестре операторов, осуществляющих обработку ПДн.

## 5. Уведомление об инцидентах

В КГОБУ Владивостокская КШ IV вида в соответствии со ст. 19 ФЗ «О персональных данных» необходимо проводить обнаружение фактов несанкционированного доступа к персональным данным и принятие мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных

атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них.

КГОБУ Владивостокская КШ IV вида обязано в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, КГОБУ Владивостокская КШ IV вида обязано с момента выявления такого инцидента уведомить уполномоченный орган по защите прав субъектов персональных данных:

1) в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

2) в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

## 6. Структура системы обеспечения информационной безопасности КГОБУ Владивостокская КШ IV вида

В КГОБУ Владивостокская КШ IV вида объектами, подлежащими защите от угроз безопасности информации (объектами защиты), являются:

– *защищаемая информация (ПДн, учетные данные пользователей, данные о конфигурации информационной системы);*

– *узел вычислительной сети, включая:*

- *автоматизированные рабочие места;*

- *виртуальные серверы*

– *программно-аппаратные средства*[1] *обработки и хранения ПДн, включая:*

- *съемные машинные носители информации;*
- *машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках)*

– *сетевой трафик;*

– *средство защиты информации;*

– *сетевое (телекоммуникационное) оборудование;*

– *сетевое программное обеспечение;*

– *системное программное обеспечение;*

– *прикладное программное обеспечение (далее в настоящем документе рассмотрено в составе узлов: АРМ и виртуальных серверов);*

– *обеспечивающие системы.*

Для обеспечения безопасности информации в КГОБУ Владивостокская КШ IV вида функционирует система обеспечения информационной безопасности, в рамках которой реализованы правовые, организационные, технические и иные меры, направленные на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к прекращению
или нарушению функционирования компонентов *ИС* и обеспечивающих (управляемого, контролируемого) им процессов, а также нарушению безопасности обрабатываемой информации (нарушению доступности, целостности, конфиденциальности информации) и обеспечивающие устойчивое функционирование компонентов *ИС* при проведении в отношении него компьютерных атак.

Система обеспечения информационной безопасности включает силы обеспечения информационной безопасности и используемые ими средства обеспечения информационной безопасности.

К силам обеспечения информационной безопасности относятся:

– Ответственный за обеспечение безопасности ПДн;

– Ответственный за обработку ПДн;

– Администратор информационной безопасности;

– подразделения (работники), эксплуатирующие «*ИС*»;

– подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) компонентов «*ИС*».

[1] Имеющие объекты файловой системы

*К средствам обеспечения информационной безопасности относятся программные и программно-аппаратные средства, применяемые для обеспечения информационной безопасности: средства защиты информации, в том числе средства защиты информации от несанкционированного доступа (включая встроенные в общесистемное, прикладное программное обеспечение), межсетевые экраны, средства обнаружения (предотвращения) вторжений (компьютерных атак), средства антивирусной защиты, средства (системы) контроля (анализа) защищенности, средства управления событиями безопасности, средства защиты каналов передачи данных.*

## 7. Меры по обеспечению безопасности информации КГОБУ Владивостокская КШ IV вида

Система обеспечения информационной безопасности должна соответствовать уровню защищенности ПДн, а также обеспечивать нейтрализацию актуальных угроз безопасности информации применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях.

КГОБУ Владивостокская КШ IV вида вправе привлекать юридических лиц, имеющих соответствующие лицензии ФСТЭК России для осуществления деятельности по технической защите информации, в том числе по внедрению СЗИ.

Состав подлежащих реализации организационных и технических мер по обеспечению безопасности информации определяется и обосновывается на этапе проектирования системы обеспечения информационной безопасности.

В целях обеспечения безопасности информации в «*ИС*» реализуются следующие меры:

- *идентификация и аутентификация;*
- *управление доступом;*
- *защита машинных носителей персональных данных;*
- *регистрация событий информационной безопасности;*
- *защита межсетевого взаимодействия;*
- *антивирусная защита;*
- *анализ защищенности информации;*
- *защита технических средств;*

– *защита информационной системы, ее средств, систем связи и передачи данных;*

– *управление конфигурацией и системой обеспечения информационной безопасности;*

– *криптографическая защита информации;*

– *безопасность технических средств и помещений;*

– *повышение осведомленности по вопросам обеспечения безопасности информации;*

– *контроль порядка обработки и защиты информации.*

При использовании в «*ИС*» новых информационных технологий и выявлении дополнительных угроз безопасности информации, для которых не определены меры по обеспечению безопасности, должны разрабатываться компенсирующие меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности информации. При этом в ходе разработки организационных и технических мер по обеспечению безопасности информации должно быть обосновано применение компенсирующих мер.

Технические меры по обеспечению безопасности информации реализуются посредством использования программных и программно-аппаратных средств – средств защиты информации (в том числе встроенных в общесистемное, прикладное программное обеспечение), а также обеспечения безопасности программного обеспечения и программно-аппаратных средств.

Безопасность информации должна обеспечиваться на всех технологических этапах обработки, в том числе при проведении ремонтных и регламентных работ. Для обеспечения безопасности информации должны применяться СЗИ, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

## 8. Контроль и управление доступом пользователей к информационным ресурсам

Перечень работников, допущенных к обработке ПДн, утверждается директором КГОБУ Владивостокская КШ IV вида. Доступ работников к обработке ПДн предоставляется по согласованию с Ответственным за обеспечение безопасности ПДн.

Контроль прав доступа пользователей проводится на регулярной основе, не реже одного раза в год.

Пользователи допускаются к обработке ПДн только после прохождения инструктажа по вопросам обеспечения безопасности ПДн.

При взаимодействии КГОБУ Владивостокская КШ IV вида с юридическими и физическими лицами, при котором КГОБУ Владивостокская КШ IV вида осуществляет передачу ПДн такому лицу, должно быть оформлено соответствующее поручение на обработку ПДн этим лицом.

Надзорному органу, осуществляющему функции контроля (надзора) в области ПДн (Роскомнадзор), должны предоставляться права доступа к ПДн, обрабатываемым Учреждением, только в сфере их компетенции и в объеме, предусмотренном законодательством Российской Федерации.

Учреждением должна обеспечиваться однозначная идентификация и аутентификация субъектов доступа (внутренних, внешних) при доступе к объектам доступа.

Запрещается повторное использование пароля пользователя, а также совместное использование одного пароля несколькими пользователями.

Любые действия пользователей до прохождения процедуры идентификации и аутентификации на автоматизированном рабочем месте пользователя запрещены.

В процессе ввода пароля должно осуществляться его сокрытие посредством отображения специальных условных знаков, например, «*», «•».

В «*ИС*» должны быть предусмотрены меры своевременного блокирования доступа пользователя в случае компрометации пароля пользователя, отзыва прав доступа, нарушения политики безопасности.

В «*ИС*» должно быть ограничено количество неуспешных попыток входа, а также должно обеспечиваться блокирование сеанса доступа после установленного времени бездействия пользователя или по запросу пользователя.

Несанкционированное подключение к «*ИС*» мобильных технических средств и портативных рабочих станций запрещено.

## 9. Ограничение программной среды

В КГОБУ Владивостокская КШ IV вида должен быть определен перечень компонентов ПО (состава и конфигурации), подлежащих установке после загрузки операционной системы.

Параметры установки компонентов ПО должны исключать установку компонентов ПО, использование которых не требуется для реализации

информационной технологии. При установке ПО должна быть возможность выбора конфигурации устанавливаемых компонентов ПО.

Контроль за установкой компонентов ПО (состав компонентов, параметры установки, конфигурация компонентов) осуществляется ответственными за обеспечение безопасности информации в пределах своих компетенций.

Параметры настройки компонентов ПО, включая программные компоненты СЗИ, должны обеспечивать реализацию мер защиты информации, а также устранение возможных уязвимостей, приводящих к возникновению угроз безопасности информации.

## 10. Обеспечение безопасности носителей информации

Должен быть разработан журнал машинных носителей защищаемой информации и места их хранения (далее — Перечень).

Запрещается хранить защищаемую информацию в местах, не указанных в Перечне.

Для хранения носителей информации используются специально оборудованные хранилища (сейфы, шкафы, и т.п.), исключающие возможность несанкционированного копирования информации и хищения носителей информации.

Перемещение носителей информации за пределы КГОБУ Владивостокская КШ IV вида допускается по согласованию в простой письменной форме по электронной почте с ответственными за обеспечение безопасности информации в пределах их компетенций.

В КГОБУ Владивостокская КШ IV вида должен быть определен порядок работы
с носителями защищаемой информации, который должен предусматривать порядок учета, хранения и обращения с носителями информации, а также порядок их уничтожения.

## 11. Регистрация событий информационной безопасности

К событиям безопасности, подлежащим регистрации в «*ИС*», относятся проявления состояния и системы защиты, указывающие на возможность нарушения Конфиденциальности, Целостности или Доступности информации, нарушения процедур, установленных внутренними нормативными документами КГОБУ Владивостокская КШ IV вида по защите информации, а также на нарушения штатного функционирования СЗИ. Регистрации подлежат события информационной безопасности, связанные с применением выбранных в КГОБУ Владивостокская КШ IV вида, мер по защите информации в «*ИС*».

В КГОБУ Владивостокская КШ IV вида должны быть определены правила и процедуры регистрации событий безопасности, которые должны предусматривать события безопасности, подлежащие регистрации, состав и содержание информации о событиях безопасности, сроки хранения соответствующих записей регистрационных журналов, а также защиту информации о событиях безопасности.

## 12. Защита межсетевого взаимодействия

В рамках обеспечения защиты межсетевого взаимодействия в КГОБУ Владивостокская КШ IV вида должна осуществляться фильтрация информационных потоков в соответствии со списками контроля доступа, настраиваемыми работниками на средствах межсетевого экранирования.

Маршруты, по которым разрешено передавать информацию, должны определяться, исходя из архитектуры сети и процессов обработки информации, и настраиваться работниками посредством создания списков контроля доступа на межсетевых экранах и телекоммуникационном оборудовании.

Правила управления информационными потоками должны учитывать, как минимум, адреса источника и получателя информации.

## 13. Антивирусная защита

Средства антивирусной защиты должны устанавливаться на всех рабочих станциях и серверах «*ИС*».

Средства антивирусной защиты, должны обеспечивать:

– автоматическую проверку на наличие вредоносных программ (вирусов);

– механизмы автоматического блокирования обнаруженных вредоносных программ (вирусов);

– регулярную проверку (с устанавливаемой периодичностью) на предмет наличия вредоносных программ;

– обновление базы данных признаков вредоносных компьютерных программ (вирусов).

В Учреждении должны быть определены правила и процедуры антивирусной защиты, обновления базы данных признаков вредоносных программ (вирусов), а также реагирования на вирусные заражения.

## 14. Обнаружение вторжений

В КГОБУ Владивостокская КШ IV вида должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных

на преднамеренный несанкционированный доступ к защищаемой информации, специальные воздействия на такую информацию в целях их добывания, уничтожения, искажения и блокирования доступа к ним, с использованием систем обнаружения вторжений.

Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

В КГОБУ Владивостокская КШ IV вида должны быть определены правила и процедуры обнаружения вторжений, обновления базы решающих правил.

## 15. Анализ защищенности

В КГОБУ Владивостокская КШ IV вида должны осуществляться регулярное выявление (поиск), анализ и устранение уязвимостей компонентов «*ИС*».

При выявлении (поиске), анализе и устранении уязвимостей должны проводиться:

– выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении СЗИ, правильностью установки и настройки СЗИ, технических средств и ПО, а также корректностью работы СЗИ при их взаимодействии с техническими средствами и ПО;

– разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

– анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

– устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения СЗИ, общесистемного ПО, прикладного ПО или микропрограммного обеспечения технических средств.

Контроль (анализ) защищенности информации должен осуществляться посредством контроля ПО, применяемого для обработки и защиты информации, на наличие настроек, позволяющих получать и устанавливать обновления ПО.

Контроль работоспособности (неотключения) программного обеспечения и СЗИ должен включать проверку правильности функционирования программного обеспечения и СЗИ, контроль соответствия настроек программного обеспечения и СЗИ параметрам настройки.

Ответственные за обеспечение безопасности информации в пределах своих компетенций не реже одного раза в шесть месяцев должны осуществляться контроль состава технических средств, программного обеспечения и СЗИ, применяемых в «*ИС*».

## 16. Обеспечение целостности и доступности информации

Должен осуществляться контроль целостности ПО, включая программное обеспечение СЗИ.

Контроль целостности ПО, включая программное обеспечение СЗИ, должен предусматривать:

– контроль целостности ПО СЗИ, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов СЗИ в процессе загрузки и (или) динамически в процессе работы компонентов «*ИС*»;

– контроль целостности компонентов ПО (за исключением СЗИ), исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов ПО и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы компонентов «*ИС*»;

– контроль применения средств разработки и отладки программ в составе ПО;

– регулярное тестирование функций безопасности СЗИ, в том числе с помощью тест-программ, имитирующих попытки НСД;

– обеспечение физической защиты технических средств.

Для обеспечения возможности восстановления функционирования и работоспособности компонентов «*ИС*» и средств защиты информации при возникновении аварийных ситуаций должны быть реализованы механизмы резервного копирования и восстановления информации с резервных машинных носителей.

В рамках резервного копирования должен обеспечиваться контроль результатов всех процедур резервного копирования с целью обнаружения ошибки или аварии с последующим уведомлением заинтересованных лиц.

Порядок восстановления информации с резервных машинных носителей информации (резервных копий) должен обеспечивать восстановление информации в течение установленного интервала времени.

Должны быть определены места хранения резервных копий и предприняты меры обеспечения их безопасности. Для защиты резервируемой информации также должны быть предприняты меры, обеспечивающие ее конфиденциальность, целостность и доступность.

## 17. Выявление инцидентов и реагирование на них

В Учреждении должно проводиться выявление инцидентов и реагирование на них.

Пользователи должны своевременно информировать лиц, ответственных за выявление инцидентов и реагировать на них.

При реагировании на инциденты должны осуществляться:

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

– своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них;

– 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.

## 18. Управление конфигурацией

При внесении изменений в конфигурацию компонентов «*ИС*» и систему обеспечения информационной безопасности необходимо учитывать потенциальное воздействие планируемых изменений на возникновение дополнительных угроз безопасности информации, на работоспособность «*ИС*» и систему обеспечения информационной безопасности.

Внесение изменений должно быть согласовано с ответственными за обеспечение безопасности информации в пределах своих компетенций.

Управление конфигурацией компонентов и системы обеспечения информационной безопасности должно осуществляться только ответственными за обеспечение безопасности информации, а также лицами, ответственными за администрирование и поддержку компонентов «*ИС*» и СЗИ.

## 19. Безопасность технических средств и помещений

В помещениях, в которых осуществляется обработка защищаемой информации, должен обеспечиваться режим, препятствующий возможности неконтролируемого проникновения или пребывания в помещениях, где размещены технические средства «ИС», СКЗИ, носители ключевой, аутентифицирующей и парольной информации СКЗИ, лиц, не имеющих права доступа в помещения.

Помещения должны быть оснащены входными дверьми с замками или СКУД, обеспечивающими постоянное закрытие дверей на замок и их открытия только для санкционированного прохода.

Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны. Не допускается размещение устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

## 20. Повышение осведомленности по вопросам обеспечения безопасности информации

В КГОБУ Владивостокская КШ IV вида должны быть определены следующие виды повышения осведомленности пользователей по вопросам обеспечения безопасности информации: вводный инструктаж и внеплановый инструктаж по обеспечению безопасности информации.

Вводный инструктаж должен проходить каждый работник при приеме на работу в случае, если его функциональные обязанности подразумевают обработку защищаемой информации или обеспечение функционирования компонентов «*ИС*».

Внеплановый инструктаж должен проводиться в случаях, если:

– изменились организационно-технические мероприятия по обработке и защите информации, принятые в КГОБУ Владивостокская КШ IV вида;

– изменились функциональные обязанности Пользователя, связанные с обработкой защищаемой информации;

– изменился состав программных средств для обработки защищаемой информации;

– изменился состав средств защиты информации.

Плановый и внеплановый инструктажи должны проводиться в срок не позднее 10 рабочих дней с момента принятия на работу нового работника или внесения изменений в организационно-технические мероприятия по обработке и защите информации.

Допуск работников к обработке защищаемой информации должен осуществляться только после прохождения вводного инструктажа при приеме на работу и ознакомления с внутренними нормативными документами по вопросам обработки информации и обеспечения безопасности такой информации с обязательной письменной фиксацией факта ознакомления.

## 21. Контроль порядка обработки и защиты информации

В КГОБУ Владивостокская КШ IV вида должен быть определен состав и порядок проведения мероприятий по контролю обеспечения безопасности информации при их обработке в КГОБУ Владивостокская КШ IV вида.

При выявлении нарушений требований законодательства Российской Федерации и нормативных документов КГОБУ Владивостокская КШ IV вида в отношении обработки и обеспечения безопасности информации, в том числе настоящего Положения, ответственные за обеспечение безопасности информации в пределах своих полномочий вправе инициировать служебное расследование. Результаты служебного расследования доводятся до сведения руководства для вынесения решения по факту нарушения указанных требований.

## 22. Контроль эффективности обеспечения безопасности информации

С целью поддержания безопасности «*ИС*» необходимом и достаточном уровне в КГОБУ Владивостокская КШ IV вида реализуется система регулярного контроля применяемых мер по обеспечению безопасности (мероприятия по контролю).

Ответственность за планирование и проведение контрольных мероприятий возложена на ответственных за обеспечение безопасности информации в пределах своей компетенции.

## 23. Ответственность

Работники КГОБУ Владивостокская КШ IV вида, осуществляющие обработку защищаемой информации, а также ответственные за обеспечение безопасности информации в пределах своей компетенции несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации за

нарушение требований настоящего Положения, иных внутренних нормативных документов КГОБУ Владивостокская КШ IV вида и законодательства Российской Федерации в области защиты информации.