

Государственное бюджетное дошкольное образовательное учреждение детский сад № 24 общеразвивающего вида с приоритетным осуществлением деятельности по познавательно-речевому и художественно-эстетическому развитию детей Кировского района Санкт – Петербурга

**СОГЛАСОВАНО**

Председатель ПК

\_\_\_\_\_ Фалина Л.Б.

«12» января 2021 года

**УТВЕРЖДАЮ**

Приказом № 7 п.1

Заведующий

ГБДОУ д\с №24

\_\_\_\_\_ Малич Н.П.

«12» января 2021 года

## **Положение**

### **об обеспечении безопасности автоматизированной информационной системы**

**ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ДОШКОЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ДЕТСКОГО САДА № 24 ОБЩЕРАЗВИВАЮЩЕГО ВИДА С ПРИОРИТЕТНЫМ ОСУЩЕСТВЛЕНИЕМ ДЕЯТЕЛЬНОСТИ ПО ПОЗНАВАТЕЛЬНО-РЕЧЕВОМУ И ХУДОЖЕСТВЕННО-ЭСТЕТИЧЕСКОМУ РАЗВИТИЮ ДЕТЕЙ КИРОВСКОГО РАЙОНА**

**САНКТ-ПЕТЕРБУРГА**

**2021г**

## *1. Общие положения*

Настоящее Положение определяет требования по обеспечению безопасности автоматизированной информационной системы (далее - АИС) ГБДОУ детский сад № 24 Кировского района Санкт-Петербурга (далее – Оператор).

АИС представляет собой IT-систему, предназначенную для автоматизации процессов формирования, обработки и анализа информации по основным направлениям деятельности Оператора.

Основными функциональными возможностями АИС Оператора являются:

- формирование, хранение и обновление сведений о структуре учебных подразделений Оператора;
- формирование, хранение и обновление сведений о преподавательском составе и сотрудниках учебных подразделений Оператора;
- формирование, хранение и обновление сведений об индивидуальных планах работы преподавательского состава;
- формирование, хранение и обновление сведений об учебном (учебно-производственном) плане Оператора;
- формирование, хранение и обновление сведений об учебной нагрузке преподавательского состава;
- формирование, хранение и обновление сведений о научной и учебно-методической продукции (методические рекомендации, учебные пособия, монографии, публикации) преподавательского состава;
- формирование, хранение и обновление сведений об обучающихся, проходящих обучение у Оператора;
- формирование, хранение и обновление сведений о результатах учебного процесса (итоги тестирования, экзаменов);
- аналитическая обработка информации о проведении учебного процесса как за отчётный период, так и о текущей деятельности учебных подразделений Оператора.

В качестве информации, подлежащей защите в АИС Оператора, рассматриваются:

- персональные данные преподавательского состава и сотрудников учебных подразделений;
- персональные данные обучающихся, проходящих и прошедших обучение;
- персональные данные административно-хозяйственных подразделений.

При обеспечении безопасности персональных данных в информационной системе Оператор руководствуется следующим: выбор средств защиты информации для системы защиты персональных данных; определение типа угроз безопасности персональных данных, актуальных для информационной системы; установление и обеспечение уровня защищённости персональных в информационной системе производится Оператором в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утверждённых постановлением Правительства РФ от 1 ноября 2012 г. N 1119.

Основными группами угроз, на противостояние которым направлены цели и требования безопасности, являются:

- угрозы, связанные с осуществлением несанкционированного доступа (ознакомления) с информацией, содержащей сведения о персональных данных работников и обучающихся, при ее обработке и хранении;
- угрозы, связанные с несанкционированным копированием (хищением) информации, содержащей сведения о персональных данных работников и обучающихся;

- угрозы, связанные с осуществлением доступа к информации, содержащей сведения о персональных данных работников и обучающихся, без разрешения на то ее владельца (субъекта персональных данных);
- угрозы, связанные с нарушением порядка доступа к информации, содержащей сведения о персональных данных работников и обучающихся, передаваемой заинтересованным лицам;
- угрозы, связанные с перехватом информации, содержащей сведения о персональных данных работников и обучающихся, из каналов передачи данных с использованием специализированных программно-технических средств;
- угрозы, связанные с потерей (утратой) информации, содержащей сведения о персональных данных работников и обучающихся, вследствие сбоев (отказов) программного и аппаратного обеспечения;
- угрозы, связанные с внедрением компьютерных вирусов и другого вредоносного программного обеспечения;
- угрозы, связанные с осуществлением несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.).

Функциональные требования безопасности охватывают:

- требования к осуществлению аудита безопасности;
- требования к обеспечению подлинности субъектов обмена информацией;
- требования к криптографической поддержке;
- требования к защите информации, содержащей сведения о персональных данных работников и обучающихся;
- требования к идентификации и аутентификации пользователей АИС;
- требования к управлению безопасностью;
- требования к защите системы безопасности.

## ***2. Основные функциональные возможности АИС, связанные с обеспечением безопасности (защитой информации)***

### **2.1. Защита данных пользователя**

АИС должна осуществлять функции и политику избирательного (дискреционного) управления доступом. Избирательное управление доступом должно предоставлять возможность ограничивать и контролировать доступ к системе и к информации, содержащей сведения о персональных данных.

Каждый Пользователь, пытающийся получить доступ к АИС, сначала должен проходить процедуру идентификации и аутентификации, а затем, при попытках получения доступа к активам, – авторизацию, т.е. проверку разрешений Пользователя по отношению к какому-либо защищаемому активу.

В АИС доступ к информации должен быть разрешен только уполномоченным на это Пользователям. Модель защиты АИС должна включать компоненты, которые реализуют контроль субъектов доступа, действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый объект доступа, представленный в АИС, должен быть однозначно ассоциирован с набором атрибутов безопасности, определяющих безопасность защищаемого объекта. Данный набор атрибутов должен формироваться при создании объекта и впоследствии может меняться. Изменение их значений должно быть обеспечено

только Пользователям, имеющим статус владельца объекта, а также субъектам, которым предоставлены соответствующие полномочия.

Права доступа субъектов к объекту должны определяться посредством списка управления доступом. Список управления доступом должен включать перечень пользователей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

## **2.2. Аудит событий безопасности**

АИС должна обеспечивать набор средств аудита, предназначенных для мониторинга и обнаружения нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в системе. Мониторинг относящихся к безопасности событий должен позволять обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к АИС или доступа к защищаемой информации. В частности, определяя политику аудита, уполномоченный администратор АИС должен иметь возможность осуществлять аудит только необходимых типов событий безопасности, таких как неудачные попытки подключения пользователей к АИС. Запись результатов аудита событий безопасности должна осуществляться в журналы регистрации событий аудита, доступ к которому должен быть разрешен только уполномоченному администратору АИС. Просмотр журналов регистрации событий аудита должен выполняться с использованием средств АИС (специализированных инструментальных средств). Данные средства должны предоставлять возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволит ограничить объем данных, собираемых о событиях безопасности.

## **2.3. Идентификация и аутентификация**

АИС должна требовать, чтобы все субъекты доступа уникально идентифицировались и аутентифицировались при доступе к АИС с помощью ввода идентификатора и пароля. Идентификация и аутентификация должны осуществляться до выполнения субъектом доступа каких-либо действий. АИС должна поддерживать аутентификацию Пользователей вместе с их авторизацией. Предусматривается, что авторизация Пользователей представляет начальный уровень для разрешения доступа к локальным и сетевым ресурсам.

АИС должна обеспечивать хранение паролей в преобразованном формате. АИС должна предоставлять средства усиления безопасности паролей через использование механизмов, позволяющих определить минимальную длину, время действия (минимальное и максимальное), задать требование уникальности (неповторяемости) и время смены пароля.

АИС должна предоставлять механизм блокирования учетной записи пользователя после определенного количества попыток ввода неправильного имени и/или пароля пользователя до ее разблокирования администратором АИС или по истечении времени действия, заданного для счетчика блокировки.

## **2.4. Защита системы безопасности**

АИС должна предоставлять ряд возможностей для обеспечения защиты системы безопасности. Изоляция процессов и поддержания домена безопасности должны обеспечивать безопасное выполнение функций системы безопасности АИС. Возможность осуществления периодического тестирования среды функционирования АИС (аппаратной части) и собственно самих функций системы безопасности АИС должно обеспечивать поддержание уверенности администратора АИС в целостности и корректности функционирования функций системы безопасности.

### **3. Основные функциональные возможности повышения надежности**

АИС должна обеспечивать надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.

#### **3.1. Резервное копирование данных**

В АИС должны входить стандартные средства предотвращения потери данных и их восстановления в случае возможных сбоев. Имеющиеся средства резервного копирования должны предоставлять Пользователям возможность выбора различных стратегий резервного копирования, обеспечивающих необходимый уровень защиты данных в случае возникновения сбоев в работе системы, при этом Пользователям должна предоставляться возможность выполнения резервного копирования данных на несъемные и съемные устройства хранения.

#### **3.2. Восстановление системы**

Функциональные возможности восстановления системы должны позволять возвращать АИС в состояние, предшествующее сбою. При этом в АИС не должно происходить потери (либо потери должны быть минимальны) и искажения данных.

#### **3.3. Средства администрирования, управления и поддержки**

В состав АИС должны быть интегрированы графические средства администрирования и/или утилиты командной строки, обеспечивающие эффективное полномасштабное и гибкое управление (в том числе мониторинг).

## **4. Среда безопасности АИС**

### **4.1. Модели угроз, характерные для АИС**

4.1.1. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся.

**Источники угрозы** – внешний злоумышленник.

**Способ (метод) реализации угрозы** – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств.

**Используемые уязвимости** – возможные недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления с передаваемой информацией третьих лиц.

**Вид информации, потенциально подверженной угрозе** – персональные данные работников и обучающихся.

**Нарушаемое свойство безопасности** – конфиденциальность.

**Возможные последствия реализации угрозы** – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации. Нанесение косвенного материального ущерба образовательному учреждению.

4.1.2. Осуществление несанкционированного ознакомления с персональными данными работников и обучающихся и их модификация (в том числе подмена).

**Источники угрозы** – внешний злоумышленник.

**Способ (метод) реализации угрозы** – перехват информации из каналов передачи данных с использованием специализированных программно-технических средств; модификация (в том числе подмена) перехваченной информации и навязывание ложной информации.

**Используемые уязвимости** – недостатки механизмов защиты информации при ее передаче по каналам передачи данных, связанные с возможностью несанкционированного ознакомления и модификации (в том числе подмены) передаваемой информации.

**Вид информации, потенциально подверженной угрозе** – персональные данные работников и обучающихся.

**Нарушаемые свойства безопасности** – конфиденциальность, целостность.

**Возможные последствия реализации угрозы** – нанесения морального и/или материального ущерба лицу, фигурирующему в перехваченной информации из-за несанкционированного раскрытия конфиденциальной информации или распространения раскрытых данных. Нанесение косвенного материального ущерба образовательному учреждению.

4.1.3. Нарушение доступности, утрата или искажение предоставляемых персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения.

**Источники угрозы** – программное и аппаратное обеспечение.

**Способ (метод) реализации угрозы** – сбои (отказы) программного и аппаратного обеспечения.

**Используемые уязвимости** – недостатки механизмов обеспечения доступности требуемой информации, связанные с возможностью блокирования предоставления информации на недопустимое время.

**Вид информации, потенциально подверженной угрозе** – персональные данные работников и обучаемых.

**Нарушаемое свойство безопасности** – доступность, достоверность.

**Возможные последствия реализации угрозы** – нарушение со стороны образовательного учреждения взятых на себя обязательств по обработке персональных данных работников и обучающихся и может привести к прямому или косвенному материальному ущербу образовательному учреждению.

4.1.4. Нарушение согласованности данных в персональных данных работников и обучающихся вследствие сбоев (отказов) программного и аппаратного обеспечения, а также ошибок персонала образовательного учреждения.

**Источники угрозы** – программное и аппаратное обеспечение, персонал образовательного учреждения.

**Способ (метод) реализации угрозы** – сбои (отказы) программного обеспечения и ошибки персонала образовательного учреждения.

**Используемые уязвимости** – недостатки механизмов обеспечения согласованности данных в БД АИС, связанные с возможностью нарушения согласованности.

**Вид информации, потенциально подверженной угрозе** – персональные данные работников и обучающихся.

**Нарушаемые свойства безопасности активов** – достоверность, целостность.

**Возможные последствия реализации угрозы** – рассогласование в персональных данных работников и обучаемых, хранимых в БД АИС, что, в свою очередь, приведет к возможному нанесению морального и/или материального ущерба образовательному учреждению.

4.1.5. Осуществление доступа (ознакомления) с персональными данными обучающегося, хранимыми и обрабатываемыми в АИС, без согласия субъекта персональных данных или окончания срока действия такого согласия.

**Источники угрозы** – уполномоченные на доступ к персональным данным внутренние и внешние пользователи.

**Способ (метод) реализации угрозы** – осуществление доступа к персональным данным обучающихся с использованием штатных средств, предоставляемых программно-аппаратным обеспечением АИС.

**Используемые уязвимости** – недостатки механизмов защиты персональных данных обучающегося, связанные с возможностью доступа к ним без письменного согласия субъекта персональных данных или после окончания срока его действия.

**Вид информации, потенциально подверженной угрозе** – персональные данные обучающихся.

**Нарушаемые свойства безопасности** – конфиденциальность.

**Возможные последствия реализации угрозы** – несанкционированное ознакомление с персональными данными ведет к нанесению морального и/или материального ущерба обучающемуся из-за несанкционированного раскрытия конфиденциальной информации.

4.1.6. Внедрение в информационную систему образовательного учреждения вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами, а также пользователями с носителей информации, используемых на автоматизированных рабочих местах.

**Источники угрозы** – внутренние пользователи и персонал образовательного учреждения, внешние системы.

**Способ (метод) реализации угрозы** – внедрение вирусов и другого вредоносного программного обеспечения при взаимодействии с внешними системами (файловый обмен, электронная почта и т.п.), а также при использовании съемных носителей информации на автоматизированных рабочих местах.

**Используемые уязвимости** – недостатки механизмов защиты информационной системы образовательного учреждения от внедрения вирусов и другого вредоносного программного обеспечения, связанные с возможностью внедрения вирусов и другого вредоносного программного обеспечения.

**Вид информации, потенциально подверженной угрозе** – программное обеспечение информационной системы образовательного учреждения.

**Нарушаемое свойство безопасности активов** – целостность.

**Возможные последствия реализации угрозы** – нарушение режимов функционирования информационной системы образовательного учреждения, потеря (утрата) и искажение информации, снижение уровня защищенности информационной системы образовательного учреждения. Ведет к возможному материальному ущербу образовательному учреждению.

4.1.7. Осуществление несанкционированных информационных воздействий (модификация конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.) на информационную систему образовательного учреждения, осуществляемых из внешних систем.

**Источники угрозы** – внешние злоумышленники, внешние системы.

**Способ (метод) реализации угрозы** – несанкционированные информационные воздействия с использованием специализированного программно-аппаратного обеспечения.

**Используемые уязвимости** – недостатки механизмов защиты информационной системы образовательного учреждения от несанкционированных внешних воздействий.

**Вид информации, потенциально подверженной угрозе** – программно-аппаратное обеспечение информационной системы образовательного учреждения.

**Нарушаемые свойства безопасности активов** – конфиденциальность, целостность.

**Возможные последствия реализации угрозы** – нарушение режимов функционирования информационной системы образовательного учреждения, снижение уровня защищенности информационной системы образовательного учреждения. Ведет к возможному материальному ущербу образовательному учреждению.

#### **4.2. Политика и цели безопасности для АИС**

АИС должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть обеспечена регистрация и учет получения (включая указание срока действия) согласия обучающегося на обработку предоставленных им в образовательное учреждение своих персональных данных.
2. Должна быть обеспечена возможность надежного хранения персональных данных работников и обучающихся (в течение действия срока трудового договора и разрешения на обработку персональных данных соответственно).
3. Должна быть обеспечена возможность безопасного восстановления АИС после сбоев и отказов программного обеспечения и оборудования.
4. Должна быть обеспечена защита информации, составляющей персональные данные работников и обучающихся, при ее обработке, хранении и передаче специализированными средствами защиты.
5. Должно быть обеспечено наличие надлежащих, защищенных от несанкционированного использования, механизмов регистрации и предупреждения администратора АИС о любых событиях, относящихся к безопасности АИС.
6. Должно быть обеспечено наличие надлежащих и корректно функционирующих средств администрирования безопасности информационной системы образовательного учреждения, доступных только уполномоченным администраторам.
7. Должны быть предоставлены механизмы аутентификации, обеспечивающие адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с низким потенциалом нападения.
8. Должны быть обеспечены механизмы генерации, надлежащего и защищенного распределения, уничтожения ключевой информации, а также механизмы шифрования, и формирования электронной цифровой подписи. Данные механизмы должны функционировать в соответствии с сертифицированными алгоритмами.

#### **4.3. Политика и цели безопасности для среды функционирования АИС**

Среда функционирования АИС должна обеспечить следование приведенным ниже правилам безопасности:

1. Должна быть обеспечена инженерно-техническая укрепленность объектов размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных.



2. Объекты размещения системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должны быть оборудованы системой охранной сигнализации.
3. Должна быть исключена возможность несанкционированного физического доступа к программно-аппаратным элементам системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, со стороны посторонних лиц.
4. На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено наличие и надлежащее использование средств антивирусной защиты, сертифицированных по требованиям безопасности. Должно быть обеспечено регулярное обновление антивирусных баз.
5. Объекты системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть подключены к внешним вычислительным сетям общего пользования с использованием надлежащих средств межсетевого экранирования, сертифицированных по требованиям безопасности.
6. На объектах системы обработки, хранения и передачи информации, содержащей сведения о персональных данных, должно быть обеспечено отсутствие нештатных программных средств, не имеющих отношения к процессу функционирования образовательного учреждения.
7. Должны быть обеспечены установка, конфигурирование и управление программно-аппаратными средствами АИС в соответствии с руководствами и согласно оцененным конфигурациям.
8. Персонал, ответственный за администрирование АИС, должен быть благонадежным и компетентным, и руководствоваться в своей деятельности соответствующей документацией.
9. Уполномоченные на работу с АИС операторы должны быть благонадежными, руководствоваться в своей работе эксплуатационной документацией на АИС, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.