Государственное бюджетное учреждение дополнительного образования
Центр творчества и образования Фрунзенского района Санкт-Петербурга
(ГБУ ДО ЦТиО Фрунзенского района Санкт-Петербурга)

УТВЕРЖДАЮ
Директор
_____ В.В. Худова
«___» _____ 20___ г.

Документ подписан электронной подписью
31.12.2022 10:11:37 (МСК)

Пользователь: Худова Виктория Валентиновна, Директор
Сертификат:
03c67485ff245a7714d4027bcab2df120b4c21f5
Выдан: Казначейство России
Период действия сертификата: 18.01.2022 по 18.04.2023

Политика информационной безопасности

Государственного бюджетного учреждения дополнительного образования
Центра творчества и образования Фрунзенского района Санкт-Петербурга

На 16 листах

Санкт-Петербург
2023

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аутентификация	–	Действия по проверке подлинности субъекта доступа в информационной системе
Безопасность информации	–	Состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность
Государственная информационная система	–	Информационная система, создаваемая в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях
Доступ к информации	–	Возможность получения информации и ее использования
Доступность	–	Состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия
Защита информации от несанкционированного доступа	–	Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации
Защищаемая информация	–	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
Идентификация	–	Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
Информационная система	–	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Информация	–	Сведения (сообщения, данные) независимо от формы их представления
Конфиденциальность	–	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
Обработка персональных данных	–	Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных
Персональные данные	–	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу
Угроза безопасности информации	–	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее
Уязвимость	–	Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть

	использована для реализации угроз безопасности информации
Целостность	− Устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ГОСТ Р	− Государственный стандарт Российской Федерации
Политика	− Политика информационной безопасности Санкт-Петербургского государственного унитарного предприятия «Санкт Петербургский информационно аналитический центр»
ГБУ ДО ЦТиО	− Государственное бюджетное учреждение дополнительного образования Центр творчества и образования Фрунзенского района Санкт-Петербурга
ФСБ России	− Федеральная служба безопасности Российской Федерации
ФСТЭК России	− Федеральная служба по техническому и экспортному контролю

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика является документом, определяющим направления деятельности в области обеспечения информационной безопасности и представляет собой систематизированное изложение целей и задач информационной безопасности, как одно или несколько правил, процедур, практических приемов и руководящих принципов, которыми руководствуется ГБУ ДО ЦТиО, а также организационных, технологических и процедурных аспектов обеспечения информационной безопасности.

Положения настоящей Политики не распространяются на обеспечение информационной безопасности сведений, составляющих государственную тайну.

Основной задачей в области информационной безопасности ГБУ ДО ЦТиО признает совершенствование мер и средств обеспечения защиты информации информационных ресурсов ГБУ ДО ЦТиО в контексте развития законодательства Российской Федерации и норм регулирования информационной деятельности в текущих условиях функционирования информационного поля.

При разработке Политики учитывались основные принципы создания систем защиты информации, характеристики и возможности организационно-технических мер и современных программных и аппаратно-программных средств защиты информации.

В рамках своей деятельности ГБУ ДО ЦТиО обязуется предпринимать все возможные меры для защиты информации от угроз безопасности информации.

Требования информационной безопасности, соответствуют целям деятельности ГБУ ДО ЦТиО и предназначены для снижения рисков, связанных с реализацией угроз безопасности информации.

Политика доступна всем работникам ГБУ ДО ЦТиО и всем пользователям его ресурсов.

2 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Субъекты информационный отношений

Субъектами при обеспечении информационной безопасности в ГБУ ДО ЦТиО являются:

работники структурных подразделений (в том числе уволенные);

физические лица, представители контрагентов в рамках исполнения договорных обязательств;

физические лица, подавшие обращение в адрес ГБУ ДО ЦТиО;

юридические лица, в рамках исполнения договорных обязательств или во исполнении требований со стороны законодательства Российской Федерации;

органы государственной власти.

Объекты информационных отношений

Объектами информационных отношений являются:

информационные ресурсы ГБУ ДО ЦТиО;

процессы обработки информации в информационных системах ГБУ ДО ЦТиО, процедуры сбора, обработки, хранения и передачи информации;

системы и средства защиты информации, объекты и помещения, в которых размещены средства обработки информации.

Цели обеспечения информационной безопасности

– защита интересов ГБУ ДО ЦТиО, работников и иных субъектов информационных отношений, взаимодействующих с ГБУ ДО ЦТиО, от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем ГБУ ДО ЦТиО, нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;

– обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов ГБУ ДО ЦТиО;

– соблюдение правового режима использования массивов и программ обработки информации;

– предотвращение реализации угроз безопасности для деятельности ГБУ ДО ЦТиО.

Задачи обеспечения информационной безопасности

Достижение целей обеспечения информационной безопасности и свойств информации, ГБУ ДО ЦТиО решается следующими задачами:

защиты от несанкционированного доступа к информационным ресурсам;

разграничения доступа пользователей к информационным, аппаратным, программным и иным ресурсам;

контроля целостности среды исполнения программ и ее восстановление в случае нарушения;

обеспечения аутентификации и идентификации пользователей, участвующих в информационном обмене;

обеспечения исправности применяемых в информационных системах ГБУ ДО ЦТиО средств защиты информации;

своевременного выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;

созданием условий для минимизации наносимого ущерба неправомерными действиями, и устранение последствий нарушения информационной безопасности в Комитет.

3 ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение информационной безопасности, должно осуществляться в соответствии со следующими основными принципами:

Принцип законности

При выборе мероприятий по защите информации, должно соблюдаться действующее законодательство Российской Федерации в сфере защиты информации.

Все работники должны иметь представление об ответственности за правонарушения в сфере защиты информации. Программно-аппаратные средства, применяемые в ГБУ ДО ЦТиО, должны иметь соответствующие лицензии, официально приобретаться у представителей разработчиков этих средств или являться интеллектуальной собственностью ГБУ ДО ЦТиО.

Принцип системности

При создании системы защиты должны учитываться актуальные угрозы безопасности информации, возможные объекты и направления атак на нее со стороны нарушителей. Система защиты должна строиться с учетом не только известных каналов утечки информации, но и с учетом возможности появления новых уязвимостей в программном обеспечении.

Принцип комплексности

Комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты, перекрывающей все существенные угрозы безопасности информации. Защита должна строиться эшелонировано. Физическая защита должна обеспечиваться физическими средствами и организационными мерами.

При построении, внедрении и эксплуатации системы защиты информации руководство ГБУ ДО ЦТиО обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

Принцип ответственности

Возложение ответственности за обеспечение безопасности информации и ее обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения был известен нарушитель.

Принцип профессионализма

Реализация мер защиты информации и эксплуатация средств защиты информации должна осуществляться профессиональными специалистами.

Привлечение специализированных организаций к разработке средств и реализации мер защиты информации, подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и лицензии на право оказания услуг в этой области.

Принцип минимизации привилегий пользователей

Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих должностных обязанностей в ГБУ ДО ЦТиО.

4 ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Система защиты информации должна предусматривать комплекс организационных, программных и программно-аппаратных средств и мер по защите информации в процессе ее обработки.

Выполнение требований достигается за счет реализации на объектах информатизации мер по защите информации:

идентификации и аутентификации субъектов доступа и объектов доступа;

управлению доступом субъектов доступа к объектам доступа;

ограничению программной среды;

защите машинных носителей персональных данных;

регистрации событий безопасности;

антивирусной защите;

обнаружению вторжений;

контролю (анализу) защищенности персональных данных;

обеспечению целостности информационной системы и персональных данных;

обеспечению доступности персональных данных;

защиты технических средств;

защиты информационной системы, ее средств, систем связи и передачи данных;

выявлению инцидентов и реагирование на них;

управлению конфигурацией информационной системы и системы защиты персональных данных.

ГБУ ДО ЦТиО, как обладатель информации ограниченного доступа, при осуществлении своих прав обязано:

соблюдать права и законные интересы иных лиц;

принимать необходимые меры по защите информации;

ограничивать доступ к информации, если такая обязанность установлена законодательством Российской Федерации.

В том числе ГБУ ДО ЦТиО, вправе если иное не предусмотрено законодательством Российской Федерации:

разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

использовать информацию, в том числе распространять ее, по своему усмотрению;

передавать информацию другим лицам на установленном законодательством Российской Федерации основании;

защищать установленными законодательством Российской Федерации способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

осуществлять иные действия с информацией или разрешать осуществление таких действий, если эти действия не противоречат федеральным законам и другим нормативно-правовым актам Российской Федерации.

Защита информации ограниченного доступа представляет собой принятие организационных и технических мер, направленных на:

соблюдение конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);

обеспечение целостности информации (исключение неправомерного уничтожения или модифицирования информации);

реализацию права на доступ к информации (исключение неправомерного блокирования информации).

Организация защиты информации

При организации в ГБУ ДО ЦТиО защиты информации, должны выполняться требования Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации. В

том числе требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах утвержденные приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для государственных информационных систем по которым ГБУ ДО ЦТиО является Оператором.

В ГБУ ДО ЦТиО помимо реализации основных мер защиты информации осуществляется:

информирование, обучение и повышение квалификации работников ГБУ ДО ЦТиО в сфере информационной безопасности;

методическая помощь работникам в вопросах обеспечения информационной безопасности;

анализ и поиск возможностей по повышению уровня защищенности информации.

Для организации защиты информации, ГБУ ДО ЦТиО вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству Российской Федерации, меры.

В рамках обеспечения защиты информации, в рамках трудовых отношений необходимо ознакомить под роспись работников, доступ которых к информации ограниченного доступа, необходим для выполнения ими своих должностных обязанностей, с перечнем информации ограниченного доступа, и принятыми в ГБУ ДО ЦТиО мерами защиты информации.

Обеспечение безопасности персональных данных достигается, в частности:

определением угроз и нарушителей безопасности персональных данных при их обработке в информационных системах персональных данных;

определением уровня защищенности персональных данных в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

оценкой эффективности принимаемых мер по защите персональных данных до ввода в эксплуатацию информационной системы персональных данных;

восстановлением персональных данных, вследствие получения несанкционированного доступа к ним;

установлением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

контролем за принимаемыми мерами по защите персональных данных и определенного уровня защищенности информационных системах персональных данных в процессе ее эксплуатации.

Особенности защиты персональных данных

При организации в ГБУ ДО ЦТиО защиты персональных данных необходимо руководствоваться требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», который регулирует отношения, связанные с обработкой и хранением персональных данных граждан и определяет требования по защите их конфиденциальности.

ГБУ ДО ЦТиО самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом №152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом №152-ФЗ или другими федеральными законами.

Перечень мер, выполнение которых обеспечивает ГБУ ДО ЦТиО в качестве оператора персональных данных, должен включать:

– назначение в ГБУ ДО ЦТиО ответственного за организацию обработки персональных данных;

– издание ГБУ ДО ЦТиО документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

– ознакомление работников ГБУ ДО ЦТиО, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику ГБУ ДО ЦТиО в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и обучение, при необходимости, указанных работников.

– ГБУ ДО ЦТиО при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5 ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Физическая безопасность

Принятые организационные и технические меры по защите помещений ГБУ ДО ЦТиО, серверного и коммутационного оборудования, автоматизированных рабочих мест пользователей информационных систем ГБУ ДО ЦТиО обеспечивают реализацию следующих мер по:

разграничению доступа работников в помещения ГБУ ДО ЦТиО в соответствии с их полномочиями и должностными обязанностями;

Безопасность на рабочем месте

Запрещается вести запись паролей в открытом виде.

Документы и носители с информацией ограниченного доступа должны убираться в сейф при уходе с рабочего места. На автоматизированном рабочем месте Пользователя рабочая сессия должна быть прервана, рабочий стол заблокирован. Вход пользователя в систему не должен выполняться автоматически.

Размещение технических средств вывода информации в помещениях ГБУ ДО ЦТиО производится с учетом исключения возможности визуального просмотра информации посторонними лицами и работниками, не допущенным к работе с данной информацией.

Технические средства должны размещаться и храниться таким образом, чтобы сократить возможный риск повреждения и угрозы несанкционированного доступа.

Физическая безопасность и безопасность на рабочем месте

Система защиты зданий и помещений ГБУ ДО ЦТиО, объектов и технических средств информационных систем ГБУ ДО ЦТиО обеспечивает выполнение следующих функций:

- регистрацию фактов входа посторонних лиц в здания ГБУ ДО ЦТиО;
- предотвращение доступа посторонних лиц в помещения, где размещены аппаратные и сетевые ресурсы информационных систем;

Работники ГБУ ДО ЦТиО на момент своего отсутствия на рабочем месте обязаны исключить возможность наличия на рабочем столе документов или носителей с защищаемой информацией.

Помещения ГБУ ДО ЦТиО должны быть оборудованы детекторами огня и дыма, огнетушителями, средствами охранно-пожарной сигнализации.

Пользователи портативных технических средств не должны оставлять техническое оборудование и носители информации без присмотра.

Безопасность при работе с носителями информации

В ГБУ ДО ЦТиО должны соблюдаться меры по безопасной работе с электронными носителями информации с целью контроля их использования, для предотвращения несанкционированного копирования и разглашения защищаемой информации, внесения изменений или уничтожения указанной информации, а также внесения изменений в работу информационных систем.

Работники ГБУ ДО ЦТиО должны использовать электронные носители информации только для выполнения своих служебных обязанностей. Использование электронных носителей информации в ГБУ ДО ЦТиО в иных целях строго запрещено.

При снятии электронного носителя информации с эксплуатации, все данные, хранящиеся на нем, должны быть гарантированно стерты.

Техническое обслуживание оборудования

Технические средства ГБУ ДО ЦТиО должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированными специалистами.

Техническое обслуживание оборудования сторонними организациями не должно приводить к риску нарушения конфиденциальности защищаемой информации.

Контроль доступа к информационным системам

Все работники ГБУ ДО ЦТиО, допущенные к работе с информационными системами, несут персональную ответственность за нарушения установленного порядка обработки информации.

Уровень полномочий пользователя в информационной системе ГБУ ДО ЦТиО должен определяться в соответствии с его должностными обязанностями.

Идентификация и аутентификация

Доступ пользователей к информационным системам должен предоставляться только после успешного завершения идентификации, аутентификации.

Получение пользователем имени в информационной системе и пароля, которые обеспечивают доступ к информационной системе, должно осуществляться по представлению руководителя.

Антивирусная защита

В целях обнаружения и устранения вредоносных программ в ГБУ ДО ЦТиО должны использоваться средства антивирусной защиты информации.

Обязательному контролю средством антивирусной защиты информации должна подлежать любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация, хранимая съемных носителях информации.

При установке программного обеспечения или его обновления на северное оборудование должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

Контроль защищенности персональных данных

В целях исключения эксплуатации уязвимостей программного обеспечения должны проводиться работы по выявлению, анализу уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей. В том числе организация контроля установки обновления программного обеспечения, включая средств защиты информации.

Использование программного обеспечения

Выбор программного обеспечения для производственных нужд ГБУ ДО ЦТиО должен производиться в приоритете к отечественному, внесенного в Единый реестр российских программ. В случае отсутствия аналога в Едином реестре российских программ допускается использовать программного обеспечение импортного производства.

Использование средств криптографической защиты информации

Приобретение средств криптографической защиты информации ГБУ ДО ЦТиО осуществляется на основании договоров и контрактов с лицами имеющими действующую лицензию ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Использование электронной почты

Электронная почта должна использоваться в ГБУ ДО ЦТиО с целью организации обмена электронными сообщениями между работниками и субъектами информационной безопасности.

При использовании электронной почты запрещается:

обмен информацией ограниченного доступа;

предоставление доступа к электронной почте с использованием данных своей учетной записи третьим лицам;

открытие (запуск на выполнение) файлов, полученных по электронной почте или из ресурсов сети Интернет, без предварительной проверки их антивирусным программным обеспечением.

6 ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Управление рисками

Определение внутренних требований по защите информации, должны основываться на результатах проведения анализа рисков нарушения основных свойств безопасности для информационных ресурсов ГБУ ДО ЦТиО.

Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения целостности, конфиденциальности и доступности для информационных ресурсов ГБУ ДО ЦТиО.

Результатом проведения анализа рисков должен быть разработанный комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность ГБУ ДО ЦТиО при реализации той или иной угрозы безопасности информации и обеспечивающих в дальнейшем достаточный уровень защищенности информационных систем ГБУ ДО ЦТиО.

Повышение осведомленности работников

В рамках организации комплексного противодействия угрозам безопасности информации, исходящим от работников ГБУ ДО ЦТиО должна постоянно повышаться их осведомленность в области защиты информации.

Повышение осведомленности работников ГБУ ДО ЦТиО осуществляется:

по существующей в ГБУ ДО ЦТиО политике информационной безопасности;

по применяемым в ГБУ ДО ЦТиО мерам защиты информации;

по правильному использованию средств защиты информации.

Мониторинг текущего уровня информационной безопасности

Для обеспечения высокого уровня контроля в отношении системы обеспечения информационной безопасности в ГБУ ДО ЦТиО на постоянной основе должен проводиться комплексный анализ существующих защитных механизмов и возникающих инцидентов информационной безопасности, а также периодический аудит всей системы обеспечения информационной безопасности.

Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов.

При проведении контрольных мероприятий, связанных с оценкой функционирования защитных мер в ГБУ ДО ЦТиО, уполномоченные работники должны придерживаться следующих принципов:

- не нарушать функционирование текущей деятельности ГБУ ДО ЦТиО;
- действовать в соответствии с внутренними документами ГБУ ДО ЦТиО по информационной безопасности;
- не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности.

7 ЗАКЛЮЧЕНИЕ

При изменении действующего законодательства Российской Федерации в области защиты информации, а также организационно-распорядительных документов ГБУ ДО ЦТиО настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также внутренним документам ГБУ ДО ЦТиО.

Пересмотр и внесение изменений в настоящую Политику осуществляются на периодической и внеплановой основе.

8 СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2 Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3 Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

4 Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5 Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

6 Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

7 Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

8 Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

9 Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

10 ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».

11 ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты».

12 ГОСТ Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения».

13 ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства безопасности. Системы менеджмента информационной безопасности. Требования».

14 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

15 ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

16 ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети».

17 ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности».

18 ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства

обеспечения безопасности. Менеджмент риска информационной безопасности».

19 ГОСТ Р ИСО/МЭК 27004-2021 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание».

20 ГОСТ Р 51897-2021 «Менеджмент риска. Термины и определения».

21 ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения».

22 Концепция информационной безопасности исполнительных органов государственной власти Санкт-Петербурга от 20.02.2023.