	Министерство культуры Российской Федерации
	Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный институт культуры»
	Должностная инструкция
	ведущего специалиста по защите информации (отдел цифрового развития)
ДИ-140/01-2022	

УТВЕРЖДЕНА
приказом СПбГИК
от 01.11.2022 № 772-О

Система менеджмента качества

**ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ
(ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)**

№ 07

Версия 01

Дата введения 01.11.2022

Санкт-Петербург
2022



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 700AE60ACD20AF77619565DD4E8901CA157993E9
Владелец: Шукшин Сергей Иванович
Действителен: с 15.11.2021 по 15.02.2023

Санкт-Петербургский государственный институт культуры	Стр. 2 из 12
ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)	Версия: 01

Разработано начальником управления информационных технологий.
Исполнено начальником управления информационных технологий.

© ФГБОУ ВО «Санкт-Петербургский государственный институт культуры»

Настоящий документ является интеллектуальной собственностью СПбГИК и не может быть полностью или частично воспроизведён, тиражирован и распространён без разрешения ректора СПбГИК.



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 700AE60ACD20AF77619565DD4E8901CA157993E9
Владелец: Шукшин Сергей Иванович
Действителен: с 15.11.2021 по 15.02.2023

Санкт-Петербургский государственный институт культуры	Стр. 3 из 12
ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)	Версия: 01

Содержание

1. Общие положения.....	4
2. Должностные обязанности.....	7
3. Права.....	10
4. Ответственность.....	11
5. Заключительные положения	11
Лист согласования.....	12



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 700AE60ACD20AF77619565DD4E8901CA157993E9
 Владелец: Шукшин Сергей Иванович
 Действителен: с 15.11.2021 по 15.02.2023

Санкт-Петербургский государственный институт культуры		Стр. 4 из 12
ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)	Версия:	01

1. Общие положения

1.1 На должность ведущего специалиста по защите информации отдела цифрового развития принимается лицо:

– имеющее высшее образование – бакалавриат или высшее образование (непрофильное) – бакалавриат и дополнительное профессиональное образование – программы профессиональной переподготовки в области информационных технологий и стаж работы по направлению деятельности не менее 3 лет или высшее профессиональное образование (инженерно-экономическое или техническое) и дополнительное профессиональное образование в области информационных технологий и стаж работы не менее 3 лет:

– не имеющее (не имевшее) судимость, не подвергавшееся уголовному преследованию (за исключением лиц, уголовное преследование в отношении которых прекращено по реабилитирующим основаниям) за преступления против жизни и здоровья, свободы, чести и достоинства личности (за исключением незаконной госпитализации в медицинскую организацию, оказывающую психиатрическую помощь в стационарных условиях, и клеветы), половой неприкосновенности и половой свободы личности, против семьи и несовершеннолетних, здоровья населения и общественной нравственности, основ конституционного строя и безопасности государства, а также против общественной безопасности <1> государства, а также против общественной безопасности (статья 351.1. Трудового кодекса Российской Федерации);

– <1> лицо, имевшее судимость за совершение преступлений небольшой тяжести и преступлений средней тяжести против жизни и здоровья, свободы, чести и достоинства личности (за исключением незаконной госпитализации в медицинскую организацию, оказывающую психиатрическую помощь в стационарных условиях, и клеветы), семьи и несовершеннолетних, здоровья населения и общественной нравственности, основ конституционного строя и безопасности государства, а также против общественной безопасности, и лица, уголовное преследование в отношении которых по обвинению в совершении этих преступлений прекращено по не реабилитирующим основаниям, могут быть допущены к педагогической деятельности при наличии решения комиссии по делам несовершеннолетних и защите их прав, созданной высшим исполнительным органом государственной власти субъекта Российской Федерации, о его допуске к педагогической деятельности (статья 351.1. Трудового кодекса Российской Федерации);

– не имеющее неснятую или непогашенную судимость за иные умышленные тяжкие и особо тяжкие преступления, не указанные выше (статья 351.1. Трудового кодекса Российской Федерации);

– не признанное недееспособным в установленном федеральным законом порядке (статья 69 Трудового кодекса Российской Федерации);

– не имеющее заболеваний, предусмотренных перечнем, утверждаемым федеральным органом исполнительной власти, осуществляющим функции по выработке государственной политики и нормативно-правовому регулированию в области здравоохранения (статья 69 Трудового кодекса Российской Федерации).

1.2 Ведущий специалист по защите информации отдела цифрового развития должен знать:

- Конституцию Российской Федерации;
- Устав Института;
- трудовое законодательство;




ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 700AE60ACD20AF77619565DD4E8901CA157993E9
Владелец: Шукшин Сергей Иванович
Действителен: с 15.11.2021 по 15.02.2023

Санкт-Петербургский государственный институт культуры	Стр. 5 из 12
ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)	Версия: 01

- законодательство Российской Федерации о персональных данных;
- постановления Правительства Российской Федерации (далее - РФ), Министерства образования и науки РФ, Федерального агентства по образованию, определяющие направления развития автоматизации и совершенствования управления образовательным процессом на базе применения информационно-коммуникационных технологий (далее – ИКТ);
- общепрофессиональные руководящие методические материалы по созданию автоматизированных систем управления (далее – АСУ);
- руководящие методические материалы Министерства образования и науки РФ, Федерального агентства по образованию по разработке, внедрению и эксплуатации АСУ образовательными учреждениями высшего профессионального образования, использованию средств и систем в образовательном процессе;
- нормативно-техническую документацию по направлению своей деятельности;
- организационную структуру СПбГИК, назначение ее структурных единиц, их функции и задачи;
- основные положения законодательства о труде;
- положение об управлении информационных технологий (УИТ);
- состав, структуру и назначение средств и систем ИКТ СПбГИК;
- руководящие и нормативные материалы, касающиеся эксплуатации и ремонта средств и систем ИКТ СПбГИК;
- технико-эксплуатационные характеристики, конструктивные особенности, назначение и режимы работы средств и систем ИКТ СПбГИК, правила их технической эксплуатации;
- технологию автоматизированной обработки информации, виды технических носителей информации и правила их эксплуатации;
- методы разработки перспективных и годовых планов (графиков) работы и порядок составления отчетности об их выполнении;
- порядок составления заявок и отчетности по ним на проведение ремонтных работ, оборудование, запасные части, эксплуатационные материалы и другой технической документации;
- организацию ремонтного и технического обслуживания, порядок взаимодействия с организациями, осуществляющими централизованное обслуживание средств и систем ИКТ СПбГИК;
- передовой отечественный и зарубежный опыт эксплуатации и технического обслуживания средств и систем ИКТ;
- отечественный и зарубежный опыт в области технической разведки и защиты информации;
- основы экономики, научной организации труда и производства;
- правила и нормы охраны труда, производственной санитарии; техники безопасности, технической эксплуатации, пожарной безопасности, правила внутреннего распорядка;
- эксплуатационную и проектную документацию на автоматизированные системы СПбГИК;
- основные угрозы безопасности информации в автоматизированных системах;
- содержание эксплуатационной документации автоматизированных систем;


**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**
 Сертификат: 700AE60ACD20AF77619565DD4E8901CA157993E9
 Владелец: Шукшин Сергей Иванович
 Действителен: с 15.11.2021 по 15.02.2023

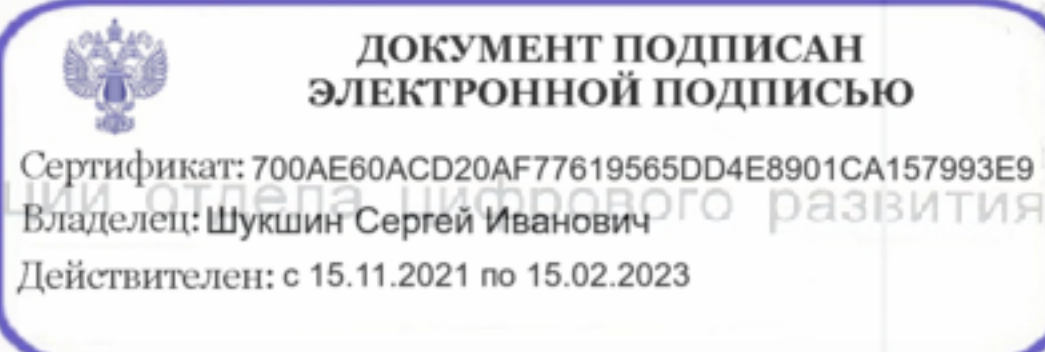
Санкт-Петербургский государственный институт культуры	Стр. 6 из 12
ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)	Версия: 01

- типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- методические и нормативные материалы по вопросам, связанным с обеспечением технической защиты информации;
- основные меры по защите информации в автоматизированных системах;
- технические средства защиты информации;
- программно-математические средства защиты информации;
- особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах;
- типовые средства, методы и протоколы идентификации, аутентификации и авторизации;
- основные методические и руководящие документы уполномоченных федеральных органов исполнительной власти по защите информации;
- порядок оформления технической документации по защите информации;
- методы анализа и защиты информации;
- типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях;
- организацию работ по защите информации;
- регламент автоматизированной системы по уничтожению информации и машинных носителей информации;
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации;
- основные методы и средства криптографической защиты информации;
- назначение и принципы работы основных узлов современных технических средств информатизации;
- каналы возможной утечки информации;
- способы защиты информации от "утечки" по техническим каналам;
- способы контроля эффективности защиты информации от "утечки" по техническим каналам;
- нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;
- организационные меры по защите информации;
- методики сертификационных испытаний технических средств защиты информации от "утечки" по техническим каналам на соответствие требованиям по безопасности информации;
- методы, способы и средства обеспечения отказоустойчивости автоматизированных информационных систем.

1.3 Ведущий специалист по защите информации отдела цифрового развития в своей работе руководствуется:

- правилами внутреннего трудового распорядка;
- кодексом этики и служебного поведения работников СПбГИК;
- положением об управлении информационных технологий;
- положением об отделе цифрового развития;
- настоящей должностной инструкцией.

1.4 Ведущий специалист по защите информации должен уметь:



Санкт-Петербургский государственный институт культуры	Стр. 7 из 12
ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)	Версия: 01

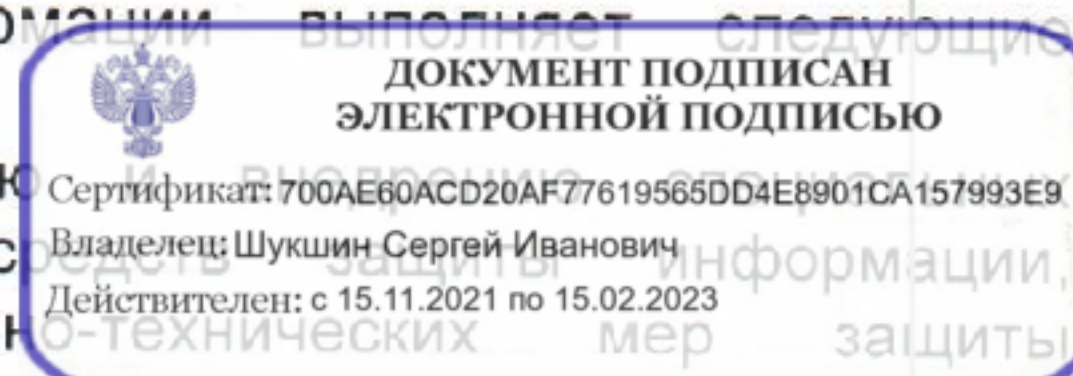
- администрировать программные средства системы защиты информации автоматизированных систем;
- устранять известные и выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации;
- применять нормативные документы по противодействию технической разведке;
- применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации;
- проводить анализ структурных и функциональных схем защищенной автоматизированной системы;
- определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы;
- применять нормативные документы по противодействию технической разведке;
- контролировать эффективность принятых мер по защите информации в автоматизированных системах;
- классифицировать и оценивать угрозы безопасности информации автоматизированной системы;
- разрабатывать предложения по совершенствованию системы управления защитой информации автоматизированной системы;
- проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств;
- реализовывать правила разграничения доступа персонала к объектам доступа;
- обучать персонал автоматизированной системы комплексу мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения защиты информации;
- осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации;
- конфигурировать аттестованную информационную систему и системы защиты информации информационной системы;
- использовать типовые криптографические средства защиты информации, в том числе средства электронной подписи;
- оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;
- использовать программные и программно-аппаратные средства для уничтожения информации и носителей информации.

1.5 Ведущий специалист по защите информации отдела цифрового развития подчиняется непосредственно начальнику отдела цифрового развития управления информационных технологий.

2. Должностные обязанности

Ведущий специалист по защите информации выполняет следующие должностные обязанности:

2.1 выполняет работу по проектированию технических и программно-математических средств обеспечения организационных и инженерно-технических мер защиты



Санкт-Петербургский государственный институт культуры	Стр. 8 из 12
ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)	Версия: 01

информационных систем, проводит исследования с целью нахождения и выбора наиболее целесообразных практических решений в пределах поставленной задачи;

2.2 осуществляет подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по техническим средствам и способам защиты информации;

2.3 участвует в рассмотрении проектов технических заданий, планов и графиков проведения работ по технической защите информации, в разработке необходимой технической документации;

2.4 составляет методики расчетов и программы экспериментальных исследований по технической защите информации, выполняет расчеты в соответствии с разработанными методиками и программами;

2.5 проводит сопоставительный анализ данных исследований и испытаний, изучает возможные источники и каналы утечки информации;

2.6 осуществляет разработку технического обеспечения системы защиты информации, техническое обслуживание средств защиты информации, принимает участие в составлении рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации, в написании и оформлении разделов научно-технических отчетов;

2.7 составляет информационные обзоры по технической защите информации;

2.8 выполняет оперативные задания, связанные с обеспечением контроля технических средств и механизмов системы защиты информации, участвует в проведении проверок учреждений, организаций и предприятий по выполнению требований нормативно-технической документации по защите информации, в подготовке отзывов и заключений на нормативно-методические материалы и техническую документацию;

2.9 готовит предложения по заключению соглашений и договоров с другими учреждениями, организациями и предприятиями, предоставляющими услуги в области технических средств защиты информации, составляет заявки на необходимые материалы, оборудование, приборы;

2.10 участвует в проведении аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности;

2.11 проводит контрольные проверки работоспособности и эффективности действующих систем и технических средств защиты информации, составляет и оформляет акты контрольных проверок, анализирует результаты проверок и разрабатывает предложения по совершенствованию и повышению эффективности принимаемых мер;

2.12 изучает и обобщает опыт работы других учреждений, организаций и предприятий по использованию технических средств и способов защиты информации с целью повышения эффективности и совершенствования работ по ее защите и сохранению государственной тайны;

2.13 выполняет работы в установленные сроки на высоком научно-техническом уровне, соблюдая требования инструкций по режиму проведения работ;

2.14 проводит регламентные работы по эксплуатации систем защиты информации автоматизированных систем;

2.15 обеспечивает работоспособность систем защиты информации при возникновении нештатных ситуаций;

2.16 мониторит защищенность информации в автоматизированных системах;

2.17 устанавливает и настраивает средства защиты информации в

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ при
Сертификат: 700AE60ACD20AF77619565DD4E8901CA157993E9
Владелец: Шукшин Сергей Иванович
Действителен: с 15.11.2021 по 15.02.2023

Санкт-Петербургский государственный институт культуры	Стр. 9 из 12
ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)	Версия: 01

автоматизированных системах;

2.18 информирует персонал о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации;

2.19 осуществляет входной контроль качества комплектующих изделий системы защиты информации автоматизированной системы;

2.20 осуществляет автономную наладку технических и программных средств системы защиты информации автоматизированной системы;

2.21 проведение приемочных испытаний системы защиты информации автоматизированной системы;

2.22 определяет правила и процедуры управления системой защиты информации автоматизированной системы, выявления инцидентов, реагирования на инциденты, мониторинга обеспечения уровня защищенности информации автоматизированной системы;

2.23 определяет правила и процедуры защиты информации при выводе автоматизированной системы из эксплуатации;

2.24 выбирает и обосновывает критерии эффективности функционирования защищенных автоматизированных систем;

2.25 проводит анализ уязвимости программных и программно-аппаратных средств системы защиты информации автоматизированной системы;

2.26 проводит экспертизу состояния защищенности информации автоматизированных систем;

2.27 подготавливает документы, определяющие правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации;

2.28 подготавливает документы, определяющие правила и процедуры контроля обеспеченности уровня защищенности информации, содержащейся в информационной системе;

2.29 подготавливает документы, определяющие правила и процедуры выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и возникновению угроз безопасности информации;

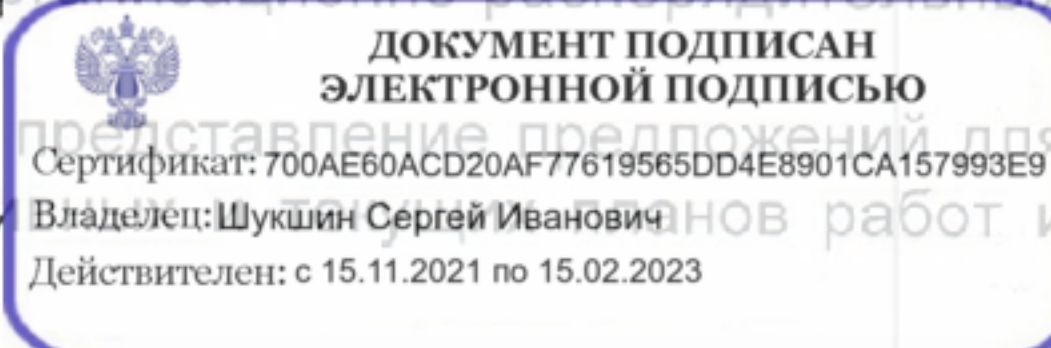
2.30 подготавливает документы, определяющие правила и процедуры управления конфигурацией аттестованной информационной системой и системой защиты информации информационной системы;

2.31 проводит сбор и анализ материалов по институту с целью выработки и принятия решений и мер по обеспечению защиты информации и эффективному использованию средств автоматического контроля, обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну;

2.32 анализирует существующие методы и средства, применяемые для контроля и защиты информации, и разрабатывает предложения по их совершенствованию и повышению эффективности этой защиты;

2.33 разрабатывает и подготавливает к утверждению проекты нормативных и методических материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;

2.34 организует разработку и своевременное включения в соответствующие разделы перспективы программ, мер по контролю и защите информации;



Санкт-Петербургский государственный институт культуры	Стр. 10 из 12
ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)	Версия: 01

2.35 дает отзывы и заключения на проекты вновь строящихся и реконструируемых зданий и сооружений и другие разработки по вопросам обеспечения защиты информации;

2.36 участвует в рассмотрении технических заданий на проектирование эскизных, технических и рабочих проектов, обеспечивает их соответствие действующим нормативным и методическим документам, а также в разработке новых принципиальных схем аппаратуры контроля, средств автоматизации контроля, моделей и систем защиты информации, оценке технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений;

2.37 выполняет отдельные служебные поручения начальника УИТ, начальника отдела цифрового развития;

2.38 незамедлительно сообщает о случаях возникновения в институте ситуации, представляющей угрозу жизни и здоровью работников;

2.39 не разглашает сведения, составляющие государственную или иную охраняемую законом тайну, ставшие известными ему в связи с исполнением своих должностных обязанностей;

2.40 бережно относится к имуществу Работодателя (в том числе к имуществу третьих лиц, находящемуся у Работодателя, если Работодатель несет ответственность за сохранность этого имущества) и других работников;

2.41 соблюдает правовые, нравственные и этические нормы, следует требованиям профессиональной этики, не допускает личной заинтересованности, которая может привести к конфликту интересов;

2.42 проходит в установленном законодательством Российской Федерации порядке обучение и проверку знаний и навыков в области охраны труда;

2.43 выполняет иные обязанности, предусмотренные законодательством Российской Федерации и Уставом института.

3. Права

Ведущий специалист по защите информации отдела цифрового развития имеет право

3.1 готовить по направлению деятельности проекты приказов, распоряжений и других правовых актов и представлять их на рассмотрение начальнику отдела цифрового развития;

3.2 запрашивать от подразделений и филиалов СПбГИК информацию в пределах своей компетенции;

3.3 обобщать, анализировать информацию, вырабатывать меры по совершенствованию работы по направлению деятельности;


3.4 вносить на рассмотрение начальника отдела цифрового развития предложения по совершенствованию и повышению эффективности системы управления информационными технологиями СПбГИК;

3.5 взаимодействовать в пределах своей компетенции с уполномоченными лицами подрядных и регулирующих организаций;

3.6 вносить предложения по изменению инструкций и организации работы

3.7 обращаться к непосредственному руководителю за разъяснениями по всем вопросам, находящимся в его компетенции;

3.8 участвовать в работе совещаний по компетенции;


ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 700AE60ACD20AF77619565DD4E8901CA157993E9
Владелец: Шукшин Сергей Иванович
Действителен: с 15.11.2021 по 15.02.2023

Санкт-Петербургский государственный институт культуры	Стр. 11 из 12
ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ВЕДУЩЕГО СПЕЦИАЛИСТА ПО ЗАЩИТЕ ИНФОРМАЦИИ (ОТДЕЛ ЦИФРОВОГО РАЗВИТИЯ)	Версия: 01

3.9 другие права, необходимые для надлежащего выполнения возложенных функций.

4. Ответственность

Ведущий специалист по защите информации отдела цифрового развития несет ответственность:

4.1 за нарушение Устава СПбГИК;

4.2 за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, в пределах, определенных действующим трудовым законодательством Российской Федерации;

4.3 за правонарушения и преступления, совершенные в процессе своей деятельности, – в порядке, установленном действующим административным, уголовным и гражданским законодательством Российской Федерации;

4.4 за правильность и полноту использования предоставленных прав;

4.5 за принятые решения;

4.6 за правильность и своевременность оформления нормативно-технической документации;

4.7 за сохранность оборудования, материалов, носителей информации, ЗИПа, инструмента, технической документации;

4.8 за рациональную организацию своего труда;

4.9 за выполнение правил и норм охраны труда, производственной санитарии, технической безопасности, технической эксплуатации, пожарной безопасности, правил внутреннего трудового распорядка;

4.10 за несоблюдение условий обеспечения сохранности документов; утрату и несанкционированное уничтожение документов;

4.11 за нарушение правил использования документов и доступа пользователей к документам, установленных законодательством Российской Федерации;

4.12 за причинение ущерба институту – в порядке, установленном действующим трудовым законодательством Российской Федерации.

5. Заключительные положения

Настоящая должностная инструкция разработана на основе: профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденным приказом Министерства труда и социального защиты Российской Федерации от 15.09.2016 N 522н;

– квалификационной характеристики должности «специалист-программист по технической защите информации, специалист-программист» (Единый квалификационный справочник должностей руководителей, специалистов и других служащих, раздел общеотраслевые квалификационные характеристики должностей работников, занятых на предприятиях, в учреждениях и организациях, утвержденный Постановлением Минтруда России от 21.08.1998 № 37).



ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 700AE60ACD20AF77619565DD4E8901CA157993E9
Владелец: Шукшин Сергей Иванович
Действителен: с 15.11.2021 по 15.02.2023