	Министерство образования Кузбасса
	Государственное профессиональное образовательное учреждение «Прокопьевский аграрный колледж»

Приложение 1
УТВЕРЖДЕНО
Приказом директора ГПОУ ПАК
№ от «___»_____2026г.

ПОЛИТИКА
ЗАЩИТЫ ИНФОРМАЦИИ

Прокопьевский район
п. Школьный
2026

СОДЕРЖАНИЕ

1	ОБЩИЕ ПОЛОЖЕНИЯ	3
2	ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ	5
3	ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ	5
4	ОБЪЕКТЫ ЗАЩИТЫ	6
5	КАТЕГОРИИ ЛИЦ, УЧАСТВУЮЩИХ В ЗАЩИТЕ ИНФОРМАЦИИ, ИХ ОБЯЗАННОСТИ (ФУНКЦИИ) И ПОЛНОМОЧИЯ	7
6	ОРГАНИЗАЦИОННАЯ СИСТЕМА УПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬЮ ПО ЗАЩИТЕ ИНФОРМАЦИИ	11
7	МЕРОПРИЯТИЯ (ПРОЦЕССЫ) ПО ЗАЩИТЕ ИНФОРМАЦИИ	13
8	МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ	13
9	ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ	15
10	ЛИСТ СОГЛАСОВАНИЯ	17
11	ЛИСТ ОЗНАКОМЛЕНИЯ	18
12	ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	20

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение и область действия документа

Настоящая Политика защиты информации (далее – Политика) определяет цели, задачи, принципы, организационную структуру и основные направления деятельности по защите информации, обрабатываемой в информационных системах (далее – ИС) Государственного профессионального образовательного учреждения «Прокопьевский аграрный колледж» (далее – Колледж).

Политика устанавливает единые подходы к формированию, функционированию и развитию системы защиты информации, а также является обязательной для применения при разработке иных локальных нормативных актов, регламентирующих вопросы информационной безопасности.

Требования Политики также обязательны для подрядных организаций и иных третьих лиц, привлекаемых к выполнению работ или оказанию услуг, связанных с доступом к ИС Колледжа либо к информации, обрабатываемой в них. Соблюдение указанных требований обеспечивается посредством включения соответствующих обязательств в договорную документацию и контроля их исполнения.

Действие настоящей Политики распространяется на:

- всех работников Колледжа независимо от занимаемой должности и характера выполняемых обязанностей, в части, касающейся их участия в обработке информации и эксплуатации ИС;
- все ИС Колледжа, а также связанные с ними сегменты сети, площадки размещения, программно-аппаратные средства и элементы информационно-телекоммуникационной инфраструктуры, перечень которых утверждается Директором Колледжа.

1.2. Нормативно-правовые акты, методические документы, национальные стандарты

Политика разработана в соответствии с:

- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (при обработке ПДн);
- Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

- Указом Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
- Приказом ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;
- Методическим документом ФСТЭК России «Мероприятия и меры по защите информации, содержащейся в информационных системах» (2026 г.);
- Трудовым кодексом Российской Федерации (в части регулирования обязанностей работников по соблюдению требований защиты информации);
- национальными стандартами Российской Федерации в области защиты информации и информационной безопасности;
- иными нормативными и методическими документами ФСТЭК России, ФСБ России, а также внутренними организационно-распорядительными документами.

1.3. Термины и определения

Термины и определения, используемые в настоящей Политике, применяются в значениях, установленных нормативными правовыми актами Российской Федерации и нормативными документами, указанными в пункте 1.2 настоящего документа.

При отсутствии специальных определений в указанных нормативных правовых актах используются термины и определения, закрепленные в национальных стандартах Российской Федерации, в том числе:

- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- ГОСТ Р 56545-2015 «Защита информации. Информация и информационные технологии. Термины и определения»;
- ГОСТ Р 56546-2015 «Защита информации. Обеспечение информационной безопасности. Термины и определения».

В случае расхождения формулировок приоритет имеют определения, установленные федеральными законами и иными нормативными правовыми актами Российской Федерации.

Использование терминов в настоящей Политике осуществляется в целях обеспечения единообразного понимания требований по защите информации и недопущения неоднозначного толкования положений документа.

2. ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

2.1. Цели защиты информации

Целью обеспечения защиты информации в Колледже является поддержание установленного уровня конфиденциальности, целостности и доступности информации, обрабатываемой в ИС, а также обеспечение устойчивости и непрерывности их функционирования посредством предупреждения и нейтрализации актуальных угроз безопасности информации и недопущения наступления неприемлемых последствий (ущерба) для деятельности Колледжа.

2.2. Задачи защиты информации

Для достижения поставленной цели защиты информации Организация решает следующие задачи:

- определение недопустимых событий, связанных с нарушением безопасности информации;
- систематическое выявление и оценка угроз безопасности информации;
- реализация организационных и технических мер защиты информации, адекватных актуальным угрозам и классу защищённости ИС;
- управление конфигурациями ИС и их уязвимостями;
- непрерывный мониторинг информационной безопасности и реагирование на инциденты;
- обеспечение физической защиты компонентов ИС;
- поддержание необходимого уровня знаний пользователей по вопросам защиты информации.

3. ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

Деятельность по обеспечению защиты информации в Колледже осуществляется на основе следующих принципов:

1. **Законность** – соблюдение требований законодательства Российской Федерации, нормативных правовых актов уполномоченных органов и локальных нормативных актов Колледжа при организации и реализации мер защиты информации.
2. **Непрерывность** – обеспечение защиты информации на всех этапах жизненного цикла ИС (проектирование, создание, ввод в эксплуатацию, эксплуатация, модернизация и вывод из эксплуатации), а также во всех режимах их функционирования.
3. **Адекватность** – соответствие применяемых мер защиты характеру актуальных угроз безопасности информации, категории и уровню защищенности ИС, а также потенциальным возможностям нарушителя.
4. **Минимизация прав и привилегий** – предоставление субъектам доступа исключительно тех прав и полномочий, которые необходимы для выполнения возложенных на них функций (принцип минимально необходимых прав, «необходимо знать»).
5. **Многоуровневость (эшелонированность)** – построение системы защиты информации по принципу последовательных и взаимодополняющих уровней защиты с использованием различных по типу и назначению средств и механизмов.
6. **Персональная ответственность** – закрепление обязанностей по обеспечению защиты информации за конкретными работниками в соответствии с их должностными обязанностями и локальными нормативными актами Колледжа.
7. **Управляемость и контролируемость** – обеспечение возможности планирования, мониторинга и оценки эффективности реализуемых мер защиты информации, а также своевременного выявления и устранения выявленных недостатков.

4. ОБЪЕКТЫ ЗАЩИТЫ

Защите подлежат:

- информационные ресурсы (информация ограниченного доступа, включая персональные данные, служебную информацию и т.д.), обрабатываемые в ИС;

- программные, программно-аппаратные и технические средства, входящие в состав ИС (серверы, автоматизированные рабочие места, сетевое оборудование, средства хранения данных, средства защиты);
- информационно-телекоммуникационная инфраструктура, на базе которой функционирует ИС (включая каналы связи, активное оборудование);
- машинные носители информации (съёмные и стационарные);
- помещения (контролируемая зона), где размещены компоненты ИС.

5. КАТЕГОРИИ ЛИЦ, УЧАСТВУЮЩИХ В ЗАЩИТЕ ИНФОРМАЦИИ, ИХ ОБЯЗАННОСТИ (ФУНКЦИИ) И ПОЛНОМОЧИЯ

5.1. Состав действующих лиц

Деятельность по защите информации в Колледже осуществляется с участием следующих категорий лиц:

- директор Колледжа;
- ответственный за организацию защиты информации;
- ответственный за защиту информации в ИС (администратор безопасности);
- ответственный за обеспечение безопасности ПДн;
- ответственный за эксплуатацию СКЗИ;
- ответственный за техническое обслуживание ИС (администратор системы);
- пользователи ИС (работники Колледжа, внешние пользователи).

Для Колледжа, отнесённой к субъектам критической информационной инфраструктуры (далее – КИИ), функции ответственного за организацию защиты информации возлагаются на заместителя директора Колледжа в соответствии с требованиями Указа Президента Российской Федерации от 01.05.2022 № 250.

Распределение обязанностей и полномочий между указанными лицами закрепляется настоящей Политикой, а также приказами директора Колледжа, должностными инструкциями и иными внутренними локальными актами Колледжа.

5.2. Обязанности (функции) и полномочия действующих лиц

5.2.1. Директор Колледжа

Основные обязанности (функции): утверждает Политику защиты информации и иные локальные нормативные акты; назначает ответственных лиц в области защиты информации; определяет структуру управления; осуществляет

ресурсное обеспечение мероприятий по защите информации; осуществляет общий контроль за состоянием защищенности; принимает решения по результатам расследований серьезных инцидентов информационной безопасности; обеспечивает взаимодействие с уполномоченными государственными органами по вопросам защиты информации.

Директор вправе: назначать ответственных лиц и допускать пользователей; утверждать внутренние локальные акты по защите информации; распределять бюджетные средства на мероприятия по защите информации; инициировать служебные проверки и применять дисциплинарные взыскания.

5.2.2. Ответственный за организацию защиты информации

Основные обязанности (функции): организует выполнение организационных и технических мер защиты; контролирует соблюдение нормативно-правовых актов; координирует деятельность работников по защите информации; организует проведение оценки состояния защиты; организует обучение работников; планирует мероприятия по повышению уровня защищенности; взаимодействует с подрядными организациями по вопросам защиты информации; докладывает руководителю о состоянии защищенности, а также о необходимости дополнительных ресурсов.

Ответственный вправе: запрашивать у подразделений информацию, необходимую для выполнения задач; давать обязательные для исполнения указания в пределах своей компетенции; инициировать служебные расследования инцидентов; приостанавливать работу ИС при выявлении критических угроз (с незамедлительным уведомлением руководителя); представлять Колледж в вопросах защиты информации перед третьими лицами; вносить предложения о совершенствовании системы защиты информации.

5.2.3. Ответственный за защиту информации в ИС (администратор безопасности)

Основные обязанности (функции): реализует организационные и технические меры защиты информации в закрепленных за ним ИС; разрабатывает и актуализирует локальные акты по защите информации в ИС; управляет учетными записями в соответствии с установленными правилами; настраивает и эксплуатирует средства защиты информации; осуществляет управление уязвимостями (выявление, устранение (нейтрализация)); контролирует конфигурации ИС, выявляет и устраняет уязвимости, управляет обновлениями

программного обеспечения; осуществляет мониторинг событий безопасности, выявляет инциденты и принимает меры по реагированию; контролирует процедуры резервного копирования; выполняет оценку показателей защищенности; уведомляет о выявленных инцидентах ответственного за организацию защиты информации.

Ответственный вправе: проводить настройку средств защиты информации; блокировать доступ пользователей при нарушении требований безопасности; требовать от пользователей соблюдения правил работы в ИС; инициировать внеочередные проверки защищенности; запрашивать у подразделений, обеспечивающих техническое обслуживание, информацию, необходимую для выполнения обязанностей; вносить предложения о совершенствовании системы защиты информации.

5.2.4. Ответственный за обеспечение безопасности ПДн

Основные обязанности (функции): разрабатывает и актуализирует локальные акты по защите ПДн; контролирует законность обработки ПДн, в том числе наличия согласий; работает с обращениями субъектов ПДн; обеспечивает конфиденциальность бумажных и электронных носителей, содержащих ПДн; информирует о нарушениях ответственного за организацию защиты информации и директора Колледжа.

Ответственный вправе: получать доступ к ИС, базам данных и документам, содержащим персональные данные, в объеме, необходимом для выполнения контрольных функций; требовать от подразделений соблюдения правил обработки ПДн; инициировать служебные проверки по фактам нарушений; представлять Колледж во взаимодействии с Роскомнадзором (при необходимости); вносить предложения о совершенствовании системы защиты ПДн.

5.2.5. Ответственный за эксплуатацию СКЗИ

Основные обязанности (функции): разрабатывает и актуализирует локальные акты по защите информации с применением СКЗИ; настраивает СКЗИ в соответствии с требованиями по эксплуатации; осуществляет ведение журналов учета СКЗИ; проводит инструктаж пользователей СКЗИ; контролирует условия эксплуатации СКЗИ; подготавливает заключения о возможности допуска пользователей к самостоятельной работе с СКЗИ, а также о возможности эксплуатации СКЗИ; информирует о нарушениях ответственного за организацию

защиты информации, ответственного за защиту информации в ИС, а также в случае серьезных нарушений директора Колледжа.

Ответственный вправе: осуществлять учет и контроль использования криптографических средств; отказывать в допуске к работе с СКЗИ при несоответствии требованиям (с незамедлительным уведомлением ответственного за защиту информации в ИС и ответственного за организацию защиты информации); инициировать замену или обновление криптографических средств; требовать соблюдения правил хранения ключевой информации; приостанавливать эксплуатацию СКЗИ при нарушении условий их применения.

5.2.6. Ответственный за техническое обслуживание ИС (администратор системы)

Основные обязанности (функции): проводит инвентаризацию активов; выполняет установку и настройку оборудования и программных средств; осуществляет обслуживание сетевого оборудования, серверов и рабочих станций; контролирует целостность программно-аппаратной среды; устраняет технические неисправности и ошибки в работе ПО; информирует о нарушениях ответственного за организацию защиты информации и ответственного за защиту информации в ИС.

Ответственный вправе: получать доступ к оборудованию и системному программному обеспечению; изменять конфигурации технических средств в рамках утвержденных процедур; приостанавливать эксплуатацию оборудования при выявлении угроз безопасности (с незамедлительным уведомлением ответственного за защиту информации в ИС и ответственного за организацию защиты информации); запрашивать у подразделений и пользователей информацию, необходимую для технического обслуживания и устранения неисправностей.

5.2.7. Пользователи ИС

Основные обязанности (функции): соблюдать требования настоящей Политики, регламентов и инструкций при работе в ИС; использовать ИС исключительно для выполнения служебных задач; сохранять конфиденциальность учетных данных (паролей, токенов) и не передавать их третьим лицам; незамедлительно уведомлять ответственного за организацию защиты информации или администратора безопасности о подозрительных событиях, попытках несанкционированного доступа, утрате носителей

информации или компрометации учетных записей; проходить инструктажи и обучение по вопросам информационной безопасности; не устанавливать несанкционированное программное обеспечение, не изменять настройки средств защиты информации.

Пользователи вправе: получать доступ к ИС, ресурсам и данным в объеме, необходимом для выполнения должностных обязанностей; использовать предоставленные программные и технические средства в соответствии с их назначением; запрашивать и получать информацию о действующих правилах обработки информации и политиках безопасности (в части, их касающейся); подавать заявки на предоставление, изменение или продление прав доступа к информационным ресурсам в установленном порядке; сообщать руководству и ответственным лицам о выявленных нарушениях, уязвимостях, инцидентах и подозрительной активности.

6. ОРГАНИЗАЦИОННАЯ СИСТЕМА УПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬЮ ПО ЗАЩИТЕ ИНФОРМАЦИИ

6.1. Организационная структура

В Колледже применяется централизованная модель управления деятельностью по защите информации, при которой стратегическое руководство осуществляется директором Колледжа, а оперативная реализация мероприятий распределяется между назначенными ответственными лицами.

Система управления деятельностью по защите информации функционирует на основе процессного подхода и принципов, изложенных в настоящей Политике, и охватывает все этапы жизненного цикла ИС.

СТРАТЕГИЧЕСКИЙ УРОВЕНЬ

Руководитель организации
Общее руководство, выделение ресурсов, утверждение политики

КООРДИНАЦИОННЫЙ УРОВЕНЬ

Ответственный за организацию ЗИ
Координация, планирование, контроль, взаимодействие с регуляторами и подрядчиками

ФУНКЦИОНАЛЬНЫЙ УРОВЕНЬ

Администратор безопасности
Настройка СЗИ, управление доступом, мониторинг инцидентов

Ответственный за СКЗИ
Учет, хранение, инструктаж по криптосредствам

Системный администратор
Техобслуживание, резервное копирование, целостность среды

Ответственный за ПДн
Контроль обработки персональных данных

ИСПОЛНИТЕЛЬНЫЙ УРОВЕНЬ

Пользователи ИС
Соблюдение правил, информирование об инцидентах

Взаимодействие: вертикальные связи (отчетность) — от исполнительного к координационному и далее к стратегическому уровню; горизонтальные связи — между функциональными специалистами. При совмещении ролей — обязательное привлечение лицензиата ФСТЭК для независимого аудита.

6.2. Механизмы взаимодействия и контроля

6.2.1. Вертикальные связи — в порядке подчиненности и отчетности: ответственный за организацию защиты информации отчитывается перед директором Колледжа; функциональные специалисты отчитываются перед ответственным за организацию защиты информации; пользователи информируют ответственных лиц о подозрительных событиях.

6.2.2. Горизонтальные связи — между функциональными специалистами: администратор безопасности взаимодействует с системным администратором; ответственный за ПДн взаимодействует с администратором безопасности; ответственный за СКЗИ взаимодействует с администратором безопасности и системным администратором.

6.2.3. Условия совмещения ролей — в целях обеспечения рационального распределения кадровых ресурсов в Колледжа допускается возложение на одного работника обязанностей по нескольким направлениям деятельности в области защиты информации. Совмещение ролей допускается исключительно при невозможности их разделения и при условии реализации компенсирующих мер, включая: участие директора Колледжа в оценке эффективности защиты; оценка состояния защиты должна проводиться с привлечением постоянно действующей комиссии; работник должен иметь необходимую квалификацию; при необходимости привлечение лицензиата ФСТЭК России.

6.2.4. Коллегиальные органы — для решения сложных вопросов и обеспечения независимой оценки директором Колледжа создается постоянно действующая комиссия по защите информации.

6.2.5. Формы контроля — мониторинг информационной безопасности (непрерывно); периодический контроль уровня защищенности (показатели Кзи, Пзи); внутренние проверки (аудиты); внешний аудит с привлечением лицензиата ФСТЭК России.

6.3. Условия привлечения лицензиата

В целях обеспечения независимой оценки состояния защиты информации Организация вправе привлекать юридическое лицо, имеющее лицензию ФСТЭК

России на деятельность по технической защите конфиденциальной информации. Привлечение лицензиата рекомендуется при: совмещении ключевых ролей; отсутствии в штате независимого компетентного специалиста по ИБ; подготовке к аттестации ИС; существенных изменениях архитектуры ИС; выявлении инцидентов ИБ; необходимости проведения оценки эффективности защиты или аттестации ИС.

7. МЕРОПРИЯТИЯ (ПРОЦЕССЫ) ПО ЗАЩИТЕ ИНФОРМАЦИИ

Обеспечение защиты информации в Колледже осуществляется на основе системного подхода и достигается не разовым применением отдельных технических или организационных средств, а посредством непрерывной реализации комплекса взаимосвязанных мероприятий (процессов), охватывающих все этапы жизненного цикла ИС — от их проектирования и ввода в эксплуатацию до модернизации и вывода из эксплуатации.

Эффективность защиты информации зависит от полноты внедрения установленных процессов, уровня компетенции работников, участвующих в их реализации, а также от актуальности и достаточности организационно-распорядительной и эксплуатационной документации.

Каждый процесс защиты информации подлежит регламентации внутренними нормативными документами Колледжа, определяющими: цели и задачи процесса; порядок выполнения мероприятий; сроки и периодичность их осуществления; формы документирования и контроля.

8. МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

8.1. Состав мер защиты

В Колледже применяются организационные и технические меры защиты информации, обеспечивающие установленный уровень защищенности и исключающие возможность совершения в отношении информации неправомерных действий, включая несанкционированный доступ, изменение, уничтожение, блокирование, копирование или распространение.

Для ИС состав и объём реализуемых мер защиты информации определяется с учетом: результатов классификации; характера обрабатываемой информации; актуальных угроз безопасности информации; особенностей архитектуры; требований нормативных правовых актов Российской Федерации.

8.2. Организационные меры

В Колледже функционирует система организационных мер защиты информации, обеспечивающая планирование, координацию, контроль и совершенствование деятельности в области информационной безопасности. Организационные меры направлены на создание управляемой системы защиты информации, в рамках которой определены структура управления, распределены обязанности и установлена персональная ответственность должностных лиц.

В целях реализации организационных мер: действует утвержденная структура управления защитой информации, включающая назначенных ответственных лиц; применяются локальные нормативные акты, регламентирующие обработку информации, порядок предоставления доступа, эксплуатацию ИС и средств защиты; осуществляется предоставление, изменение и прекращение доступа работников к информационным ресурсам в установленном порядке; проводится ознакомление работников с требованиями по защите информации и обеспечивается подтверждение их обязательств по соблюдению установленных правил; организуется регулярное обучение и инструктаж работников по вопросам информационной безопасности; осуществляется внутренний контроль соблюдения требований защиты информации, включая проведение проверок и анализ выявленных нарушений; обеспечивается документирование процессов защиты информации и хранение соответствующей документации; при привлечении подрядных организаций требования информационной безопасности закрепляются в договорных обязательствах и контролируются в ходе выполнения работ.

8.3. Технические меры

В ИС Колледжа применяется комплекс технических мер защиты информации, обеспечивающий установленный уровень защищенности и устойчивость функционирования информационной инфраструктуры. Технические меры реализуются с учетом оценки угроз, категории и уровня защищенности ИС, а также особенностей их архитектуры и эксплуатации.

В рамках реализации технических мер: обеспечивается идентификация и аутентификация пользователей и администраторов, включая применение усиленных механизмов аутентификации для привилегированных учетных записей; действует разграничение доступа к информационным ресурсам в соответствии с установленными ролями и принципом минимально необходимых

прав; осуществляется регистрация и анализ событий безопасности, обеспечивается защита журналов регистрации; применяются средства антивирусной защиты, поддерживается актуальность их баз и программных компонентов; функционируют средства межсетевого экранирования и сегментации сети, обеспечивается фильтрация сетевого трафика; используются средства обнаружения вторжений и выявления аномальной активности; осуществляется контроль целостности программных средств и конфигураций ИС; выполняется резервное копирование информации, обеспечивается хранение резервных копий и возможность восстановления данных; передача информации осуществляется с использованием защищённых протоколов и, при необходимости, средств криптографической защиты; ограничивается физический доступ к средствам обработки информации, применяются средства контроля и управления доступом в защищаемые помещения; обеспечивается устойчивость функционирования ИС, включая резервирование критически важных компонентов.

9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ

Работники Колледжа, а также иные лица, допущенные к обработке информации и эксплуатации ИС, несут ответственность за соблюдение требований законодательства Российской Федерации в области защиты информации, настоящей Политики и иных локальных нормативных актов Колледжа.

Нарушение требований о защите информации влечёт ответственность в соответствии с трудовым законодательством Российской Федерации, гражданским, административным и уголовным законодательством Российской Федерации.

Привлечение к ответственности осуществляется независимо от занимаемой должности и уровня доступа к ИС. Ответственность может наступать как при наличии наступивших негативных последствий, так и при создании угрозы их возникновения.

Основанием для привлечения к ответственности является установление факта нарушения требований о защите информации, выразившегося в: несоблюдении требований настоящей Политики; нарушении порядка обработки

информации ограниченного доступа; разглашении конфиденциальной информации; несанкционированном доступе к ИС; передаче учетных данных третьим лицам; несанкционированном изменении конфигураций; несвоевременном уведомлении о выявленных инцидентах; нарушении требований эксплуатации средств защиты информации.

Ответственные лица в области защиты информации несут персональную ответственность за: неисполнение или ненадлежащее исполнение возложенных обязанностей; отсутствие должного контроля в пределах своей компетенции; несвоевременное принятие мер по устранению выявленных нарушений; непринятие мер реагирования при выявлении инцидентов информационной безопасности. Совмещение обязанностей не освобождает должностное лицо от ответственности по каждому направлению деятельности.

ЛИСТ СОГЛАСОВАНИЯ

Ведущий юрисконсульт _____ О.А. Швец

подпись

«___» _____20___г.

Начальник ИВЦ _____ В.А.Лялин

подпись

«___» _____20___г.

ЛИСТ ОЗНАКОМЛЕНИЯ

С Политикой защиты информации ознакомлен:

Фамилия, инициалы	Дата ознакомления	Подпись

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номера страниц				Всего страниц	Дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	замененных	аннулированных	новых			