СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОАО «НОВОГРУДСКИЙ ЗАВОД ГАЗОВОЙ АППАРАТУРЫ»

(«СЗИ ИС НЗГА»)

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Новогрудок 2025 г

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ

1.1. Настоящая Политика информационной безопасности (далее – Политика) является основополагающим документом, определяющим стратегию развития информационной безопасности ОАО «Новогрудский завод газовой аппаратуры» (далее – ОАО «НЗГА»). Под информационной безопасностью ОАО «НЗГА» понимает состояние защищенности своих интересов (целей) от угроз в информационной сфере. Защищенность достигается обеспечением конфиденциальности, целостности и доступности информации.

1.2. Политика определяет цели и задачи защиты информации, которыми необходимо руководствоваться в своей деятельности, а также основные принципы построения системы управления информационной безопасностью (далее – ИБ) ОАО «НЗГА».

Настоящая Политика служит основой для разработки внутренних документов по обеспечению информационной безопасности ОАО «НЗГА».

2. ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Настоящий документ разработан в соответствии с требованиями Положения о порядке технической защиты информации в информационных системах (далее – ИС), предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 года № 66 (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 года № 195), (в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2024 г. № 259).

2.1. Нормативной правовой основой Политики информационной безопасности ИС ОАО «НЗГА» служат:

Конституция Республики Беларусь, содержащая основополагающие нормы ИБ.

Гражданский кодекс Республики Беларусь;

Уголовный кодекс Республики Беларусь;

Закон Республики Беларусь от 10 ноября 2008 года № 455-З «Об информации, информатизации и защите информации»;

Закон Республики Беларусь от 5 января 2013 года № 16-З «О коммерческой тайне»;

Закон Республики Беларусь от 28 декабря 2009 года № 113-З «Об электронном документе и электронной цифровой подписи».

Закон Республики Беларусь от 7 мая 2021 года № 99-З «О защите персональных данных».

Указ Президента Республики Беларусь от 9 декабря 2019 года № 449 «О совершенствовании государственного регулирования в области защиты информации».

Указ Президента Республики Беларусь от 16 апреля 2013 года № 196 «О некоторых мерах по совершенствованию защиты информации».

Указ Президента Республики Беларусь от 1 февраля 2010 года № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет».

Указ Президента Республики Беларусь от 8 ноября 2011 года № 515 «О некоторых вопросах развития информационного общества в Республике Беларусь».

Указ Президента Республики Беларусь от 28 октября 2021 года № 422 «О мерах по совершенствованию защиты персональных данных».

Концепция национальной безопасности Республики Беларусь, утвержденная Указом Президента Республики Беларусь от 09 ноября 2010 года № 575.

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 года № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 года № 449».

Приказ директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 года № 12 «О классификации информационных ресурсов (систем)».

Приказ директора Национального центра защиты персональных данных Республики Беларусь от 15 ноября 2021 года № 13 «Об уведомлении о нарушениях систем защиты персональных данных».

Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 года № 1 «О концепции информационной безопасности Республики Беларусь»;

иные нормативные правовые акты Республики Беларусь в области электросвязи, информатизации, безопасности и защиты информации, международные и национальные стандарты в области ИБ продуктов и систем информационных технологий.

2.2. Перечень определений, принятый в настоящем документе:

аутентификация – проверка принадлежности субъекту или пользователю предъявленного им идентификатора (например, имени пользователя и пароля, цифрового сертификата и т.д.) и предоставление соответствующих прав доступа к защищаемой информации;

доступность – свойство информации быть доступной и используемой по запросу со стороны уполномоченного пользователя;

ИБ – состояние информационной системы, при котором с требуемой вероятностью обеспечиваются конфиденциальность, целостность, подлинность, доступность и сохранность защищаемой информации;

информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

инцидент ИБ – это одно или ряд нежелательных или непредвиденных событий в области информационной безопасности, при которых имеется значительная вероятность компрометации функционирования бизнес-процессов или реализации угрозы информационной безопасности;

конфиденциальность – свойство информации, заключающееся в недоступности информации или не раскрытии ее содержания для неавторизованных лиц, процессов и логических объектов;

несанкционированный доступ – доступ к информации или воздействие на информацию, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационной системой;

пароль – набор знаков, предназначенный для подтверждения личности и (или) полномочий;

подлинность – свойство информации, гарантирующее, что информация идентична оригинальной (заявленной);

программное обеспечение (ПО) – набор команд, управляющих работой средства вычислительной техники;

система защиты информации (СЗИ) – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

сохранность – свойство информации, гарантирующее, что информация ни при каких условиях не может быть уничтожена (удалена);

угроза ИБ – совокупность условий и факторов, создающих опасность нарушения ИБ;

целостность – свойство информации, заключающееся в обеспечении точности и полноты информации.

2.3. Также применяются следующие сокращения:

АРМ – автоматизированное рабочее место.

ЗИ – защита информации.

ИС – информационная система.

ИБ – информационная безопасность.

ЛПА – локальные правовые акты.

ОАЦ – Оперативно-аналитический центр при Президенте Республики Беларусь.

ПО – программное обеспечение.

СКЗИ – средства криптографической защиты информации.

СЗИ – система зашиты информации.

3. ОБЩИЕ СВЕДЕНИЯ

3.1. Политика устанавливает общие намерения и направления деятельности по обеспечению конфиденциальности, целостности, сохранности, подлинности и доступности информации при функционировании ИС ОАО «НЗГА».

3.2. Основные положения и требования Политики обязательны для использования в работе и распространяются на специалистов, организующих и обеспечивающих эксплуатацию, обслуживание и поддержку функционирования ПО, программно-технических средств, СКЗИ, информационных ресурсов,

систем и сетей ИС ОАО «НЗГА», полный перечень которых приведен в таблице 1.

Таблица 1 – Перечень информационных ресурсов (систем) ОАО «НЗГА»

№ п/п	Информационный ресурс (система)	Типовой класс
1.	1С Управление предприятием 8.3	3-ин 3-спец
2.	«СМДО»	3-ин 3-спец
3.	ИПС Стандарт	-
4.	ИПС Эталон	-
5.	Электронный декларант	3-ин
6.	Корпоративная почта Предприятия (@novogas.by)	-
7.	Корпоративный сайт Предприятия (адрес https://novogas.by)	-

3.3. Положения Политики обязательны для исполнения всеми пользователями, имеющими доступ к информационным ресурсам и оборудованию ИС ОАО «НЗГА».

4. ЦЕЛИ И ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Целью Политики является регламентирование единых подходов и требований по обеспечению ЗИ сотрудниками (работниками) ОАО «НЗГА», а также внешними пользователями сторонних организаций при взаимодействии с ИС ОАО «НЗГА».

4.2. Достижение указанной цели предполагает решение следующих задач:

реализация требований законодательства Республики Беларусь в части ЗИ в ИС и мер контроля их защищенности;

определение ответственности субъектов информационных отношений по обеспечению и соблюдению требований Политики, в том числе с использованием программных, программно-аппаратных средств технической и криптографической защиты информации, а также посредством принятия соответствующих нормативных и организационно-методических документов по ЗИ ОАО «НЗГА»;

своевременное выявление и оценка причин, условий и характера угроз ИБ и дальнейшее прогнозирование развития событий на основе мониторинга инцидентов ИБ;

планирование, реализация и контроль эффективности использования защитных мер и средств ЗИ, создание механизма оперативного реагирования на угрозы ИБ;

реализация программ повышения осведомленности и обучения сотрудников (работников) ОАО «НЗГА» о возможных факторах рисков ИБ и мерах противодействия им.

4.3. Нарушение требований настоящего документа влечет ответственность в соответствии с законодательством Республики Беларусь.

5. ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОАО «НЗГА»

5.1. Потенциальные источники угроз ИБ ИС относятся к трем группам:

обусловленные действиями субъектов ИС – действия которых могут привести к нарушению ИБ. Данные действия могут быть как умышленными, так и случайными. В свою очередь данные источники могут быть как внешними, так и внутренними по отношению к ИС;

обусловленные программно-техническими средствами, являющимися как внутренними компонентами, так и внешними по отношению к ИС;

стихийные источники – данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия или другие обстоятельства, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить). Такие источники угроз являются внешними по отношению к ИС, под ними понимаются природные катаклизмы, техногенные катастрофы и т.п.

5.2. К субъектам ИС, действия которых способны привести к нарушению ИБ, относятся внешние и внутренние нарушители.

5.2.1. Внешние нарушители – нарушители со злонамеренными целями предпринимать атаки на ИС с целью получения доступа к ресурсам или нарушения ее функционирования. Предполагается, что внешние нарушители располагают базовым потенциалом для атаки.

Категории лиц, которые могут быть внешними нарушителями:

уволенные сотрудники;

представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энергоснабжения, водоснабжения, теплоснабжения и т.п.);

посетители;

лица, случайно или умышленно получившие доступ к ресурсам из внешних сетей.

5.2.2. Категории лиц, которыми могут быть внутренние нарушители:

зарегистрированные пользователи ИС, которые могут допускать ошибки при выполнении операций или пытаться получить доступ к ресурсам. Указанные действия проводятся из любопытства или иных побуждений, в нарушение установленных правил доступа, воспользовавшись ошибками администрирования или недостатками СЗИ. Предполагается, что зарегистрированные пользователи не обладают специальными знаниями о СЗИ, располагают базовым потенциалом для атак, стандартным (доступным) оборудованием для идентификации уязвимости и нападения;

администраторы ИС, которые могут допускать ошибки при управлении оборудованием и ПО. Предполагается, что администраторы обладают специальными знаниями о функционировании ИС, могут располагать специализированным оборудованием для идентификации уязвимости и нападения. Их действия по нападению могут иметь мотивацию;

иные нарушители, не имеющие учетной записи в ИС, но которые имеют к ИС какое-либо отношение. Действуют целенаправленно как из злонамеренных побуждений (например, корыстных интересов или мести), так и из незлонамеренных (например, любопытства). Используют набор методов и средств взлома СЗИ при базовом потенциале атаки, пассивные средства (технические средства перехвата без модификации компонентов системы), методы и средства активного воздействия (модификация технических и программных средств, подключение к каналам передачи данных, внедрение программных закладок в целях хищения, блокирования, удаления, модификации данных), а также комбинации воздействий как изнутри, так и извне – из сетей общего пользования. К указанному типу нарушителей относится технический персонал, обслуживающий здание (уборщицы, электрики, сантехники и другие работники, имеющие доступ в здание и помещения, где расположены компоненты ИС).

5.3. К программно-техническим средствам, способным повлиять на ИБ ИС, относятся внутренние и внешние компоненты ИС.

5.3.1. К внутренним программно-техническим средствам компонентов ИС, которые могут рассматриваться в качестве источников угроз ИБ ИС, относятся:

программные средства ИС;

технические средства ИС;

конфигурация ИС.

5.3.2. К внешним программно-техническим средствам по отношению к ИС относятся:

программно-технические средства среды функционирования ИС, при помощи которой осуществляется доступ как к ИС, так и к информационным ресурсам ОАО «НЗГА» через ИС;

программно-технические средства ИС ОАО «НЗГА», с которыми осуществляет взаимодействие ИС.

5.4. К стихийным источникам угроз ИБ для ИС ОАО «НЗГА» могут относиться:

пожар;

землетрясение;

наводнение;

вооруженный конфликт (как внутренний, так и внешний);

пандемия и т.п.

6. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

6.1. ОАО «НЗГА», являясь владельцем ИС, имеет право:

пользоваться, распространять, предоставлять или ограничивать доступ к информации в соответствии с законодательством Республики Беларусь;

определять порядок и условия обработки, предоставления доступа к информации, обеспечивая подключение программно-технических средств пользователей и ресурсов ОАО «НЗГА»;

осуществлять меры по защите информации;

осуществлять контроль соблюдения пользователями установленных правил доступа и использования ресурсов;

запрещать или приостанавливать обработку информации и (или) пользование ею в случае невыполнения требований по защите информации;

защищать в установленном законодательством Республики Беларусь порядке свои права в случае незаконного получения информации или незаконного пользования ею иными лицами;

осуществлять иные действия в соответствии с законодательством Республики Беларусь.

6.2. Пользователями ИС являются:

обслуживающий персонал ИС;

сотрудники (работники) ОАО «НЗГА», имеющие учетные записи в ИС;

специалисты технической поддержки оборудования и ПО (гарантийная и постгарантийная техническая поддержка согласно заключенным договорам).

6.3. Пользователи ИС имеют право:

использовать ИС для доступа к информационным ресурсам ОАО «НЗГА»

получать, накапливать и обрабатывать информацию в рамках взаимодействия с ИС;

использовать, распространять и (или) предоставлять информацию при выполнении установленных законодательством Республики Беларусь требований по ее защите.

6.4. Обслуживающий персонал ИС состоит из:

персонала, непосредственно осуществляющего эксплуатацию ИС и контроль над процессом эксплуатации (администраторы ИС, специалисты ИБ);

персонала, осуществляющего программно-техническое сопровождение и обслуживание средств ИС (специалисты, участвующие в сопровождении и не относящиеся к предыдущему абзацу).

6.5. Численность обслуживающего персонала ИС должна подбираться с учетом необходимости обеспечения непрерывности процессов обработки информации в ИС.

6.6. Обслуживающий персонал ИС обязан:

ознакомиться с требованиями настоящей Политики под роспись в листе ознакомления в приложении к настоящему документу;

выполнять требования настоящей Политики;

принимать меры по защите информации, установленные законодательством Республики Беларусь и документами ОАО «НЗГА»;

при первом входе в ИС сменить свой пароль на доступ к ИС согласно установленным правилам;

осуществлять периодическую смену своего пароля на доступ к ИС не реже, чем через 90 суток;

сообщать своему руководителю, соответствующим администраторам о фактах сбоев и отказов, а также о некорректном функционировании аппаратного и ПО ИС, в том числе средств технической защиты информации;

немедленно приостановить процесс обработки информации и сообщить соответствующему администратору ИБ ОАО «НЗГА» при подозрении на наличие вредоносного ПО или его обнаружении (сообщение антивирусной программы, необычное поведение аппаратного и (или) ПО, изменение размеров файлов и т.п.), а также в структурное подразделение, из которого поступили зараженные файлы или почтовые сообщения на своём АРМ;

в случае обнаружения неисправности в работе средства вычислительной техники или ПО, немедленно сообщать об этом системным администраторам ИС и своему руководителю, до устранения неисправностей не осуществлять работу, связанную с обработкой информации на АРМ;

обеспечивать сохранность информации, распространение и (или) предоставление которой ограничено, и не передавать ее полностью или частично иным лицам без согласия обладателя информации;

завершать сеанс связи по окончании работы, закрывать используемый браузер, а также блокировать или выключать средство вычислительной техники при оставлении рабочего места, если иное не определено технологическим процессом;

проводить удаление (уничтожение) данных с машинных носителей информации при их передаче третьим лицам, в том числе для ремонта и технического обслуживания;

ограничивать доступ к средствам вычислительной техники третьих лиц (иных пользователей, представителей сторонних организаций и т.п.);

соблюдать правила доступа в помещения, в которых установлено оборудование ИС;

на средствах вычислительной техники, которые подключаются к ИС, должно быть установлено средство защиты от вредоносного ПО, оно должно быть активировано и иметь обновленные, не реже принятых в ОАО «НЗГА» сроков обновления базы вредоносного ПО;

знать и выполнять требования по антивирусной защите;

в случае выявления вредоносного ПО немедленно сообщить об этом администратору ИБ и своему руководителю;

оказывать содействие должностным лицам ОАО «НЗГА», назначенным для проведения служебного расследования, давать необходимые пояснения, предоставлять доступ к информации, АРМ;

исполнять другие обязанности в соответствии с законодательством Республики Беларусь и документами ОАО «НЗГА».

6.7. Сотрудники ОАО «НЗГА», выделенные для поддержки работоспособности и функционирования ИС, а также обеспечения ИБ, должны обладать знаниями и навыками, необходимыми и достаточными для выполнения

возложенных на них функций, иметь квалификацию, соответствующую требованиям законодательства Республики Беларусь.

6.8. Сотрудники ОАО «НЗГА», выделенные для обеспечения ИБ, контролируют содержание всех потоков данных, проходящих через ИС предприятия.

6.9. Пользователь ИС обязан:

соблюдать права и законные интересы иных лиц при использовании ИС;

принимать меры по защите информации, установленные законодательством Республики Беларусь;

соблюдать все необходимые меры для обеспечения физической безопасности оборудования, на котором хранится информация предприятия;

при первом входе в ИС, сменить свой пароль на доступ к ИС и ее ресурсам согласно установленным правилам;

осуществлять периодическую смену своего пароля на доступ к ИС не реже, чем через 90 суток;

сообщать администраторам ИС о фактах некорректного функционирования ПО АРМ, ИС и ресурсов ОАО «НЗГА», в том числе средств технической защиты информации;

обеспечивать сохранность полученной информации, распространение и (или) предоставление которой ограничено, и не передавать ее полностью или частично иным лицам без согласия обладателя информации;

исполнять другие обязанности в соответствии с законодательством Республики Беларусь, внутренними документами ОАО «НЗГА».

6.10. Пользователям ИС запрещено:

осуществлять доступ к ИС с нарушением установленных правил;

использовать ИС и (или) АРМ в личных целях или целях, не связанных с выполнением служебных обязанностей;

разглашать пароли и иную информацию, распространение которой может повлиять на СЗИ ИС;

допускать посторонних лиц к работе на своем средстве вычислительной техники, если иное не определено технологическим процессом;

передавать посторонним лицам реквизиты доступа к ИС;

использовать реквизиты других пользователей для доступа к ИС и (или) их АРМ;

производить действия, направленные на несанкционированное получение привилегированного доступа к ИС и (или) АРМ;

проводить или участвовать в компьютерных атаках и сетевом взломе, направленных на ИС ОАО «НЗГА», АРМ сотрудников ОАО «НЗГА» или направленных против третьих лиц с использованием ресурсов АРМ и (или) ИС ОАО «НЗГА»;

самостоятельно изменять конфигурацию аппаратного и программного обеспечения, устанавливать ПО, не имеющее отношения к их производственной деятельности;

подключать к ИС ОАО «НЗГА» оборудование третьих лиц, в том числе съемные носители информации, указанное оборудование и съемные носители информации подлежат обязательной проверке сотрудником ИБ и (или) системным администратором ИС ОАО «НЗГА»;

осуществлять неправомочный доступ к АРМ и ИС ОАО «НЗГА».

7. ПЕРЕЧЕНЬ СУБЪЕКТОВ И ОБЪЕКТОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПОРЯДОК ИХ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МЕЖДУ СОБОЙ

7.1. Субъектами информационных отношений при обеспечении ИБ ИС ОАО «НЗГА» являются:

ОАО «НЗГА», в качестве обладателя информации и собственника (владельца) ИС, информационных ресурсов, информационных систем и сетей, в том числе СКЗИ;

государственные органы и организации, юридические лица, в том числе индивидуальные предприниматели, в качестве пользователей предоставляемых ОАО «НЗГА» услуг по доступу к информационным ресурсам ИС;

иные юридические лица, в том числе иностранные, международные организации, в качестве информационных посредников, операторов информационных систем и связи, поставщиков оборудования и ПО ИС (в том числе СКЗИ), а также организации, оказывающие услуги ОАО «НЗГА» по технической поддержке и осуществляющие гарантийное и сервисное обслуживание.

7.2. Ответственные и должностные лица субъектов информационных отношений (далее – представители):

должностные лица ОАО «НЗГА», осуществляющие обеспечение безопасного функционирования ИС, ПО и СКЗИ (далее – специалисты ОАО «НЗГА»);

сотрудники (работники) ОАО «НЗГА», получившие доступ к ИС посредством АРМ и пользующиеся ими в рамках выполнения своих функциональных обязанностей;

должностные лица организаций, поставляющих оборудование и ПО ИС, СКЗИ и осуществляющие их гарантийное и сервисное обслуживание;

внешние пользователи ИС – должностные лица государственных органов и организаций, юридических лиц, а также индивидуальные предприниматели, физические лица, получившие доступ к предоставляемым ОАО «НЗГА» информационным ресурсам.

7.3. Представители субъектов информационных отношений несут предусмотренную законодательством Республики Беларусь в сфере информации, информатизации и защиты информации ответственность за свои действия, если в этих действиях присутствуют признаки правонарушения.

7.4. Ответственность представителей субъектов информационных отношений за обеспечение защиты информации в ОАО «НЗГА» определяется следующими документами:

организационно-распорядительными документами ОАО «НЗГА»;

должностными инструкциями сотрудников (работников) ОАО «НЗГА»;

настоящей Политикой;

иными документами, в том числе соглашениями и договорными обязательствами при оказании услуг.

7.5. Основными объектами, на которые направлены как негативные действия в ИС, так и, соответственно, защита, являются:

информация, обрабатываемая или хранящаяся в ИС;

компоненты ИС.

7.6. Среда функционирования ИС – совокупность организационных, информационных программных и технических средств ИС при сохранении ими работоспособного состояния.

7.7. К среде функционирования ИС относятся:

внутренние документы ОАО «НЗГА», касающиеся функционирования ИС;

пользователи ИС;

средства вычислительной техники, системное и прикладное ПО пользователей и специалистов ИС;

технологическая сеть, сеть Интернет и другие сети передачи данных;

внешние ИС, в том числе их вычислительное оборудование (серверы, системы хранения данных), системное и прикладное ПО, обеспечивающее функционирование внешних ИС;

инженерные системы в серверных и служебных помещениях;

помещения, в которых размещены аппаратные средства ИС ОАО «НЗГА».

7.8. Обслуживание среды функционирования ИС обеспечивается специалистами ОАО «НЗГА» или ее контрагентами и не относится к самой ИС.

7.9. Функциональные компоненты ИС должны располагаться в помещениях, исключающих несанкционированный доступ к ним (за исключением СКЗИ подключаемых ИС), и обеспечивающих их бесперебойную круглосуточную эксплуатацию в климатических условиях, указанных в документации на эксплуатацию.

7.10. Порядок информационного взаимодействия субъектов с объектами ИС ОАО «НЗГА» должен определяться следующими документами:

внутренними документами ОАО «НЗГА»;

положениями, регламентами, порядками, инструкциями информационного взаимодействия при оказании услуг;

договорными отношениями при оказании услуг и осуществлении технической поддержки.

7.11. Порядок информационного взаимодействия объектов между собой определяется отдельной эксплуатационной (технической) документацией по ее использованию в ОАО «НЗГА» и в рамках оказания услуг.

7.12. Порядок использования ИС и управление ею (администрирование) определяются следующими документами:

регламентами (положениями, инструкциями) по эксплуатации того или иного компонента ИС;

внутренними документами ОАО «НЗГА»;

договорными отношениями при оказании услуг и в ходе осуществления технической поддержки, должностными инструкциями сотрудников (работников) ОАО «НЗГА».

7.13. Для сокращения количества разрабатываемой документации, допускается изложение положений в должностных инструкциях обслуживающего персонала ИС ОАО «НЗГА».

7.14. Специалисты, обслуживающие ИС, должны пройти обучение правилам и принципам работы с соответствующими компонентами, выполнение которых позволяет поддерживать их безопасное функционирование.

7.15. Общее руководство и ответственность за организацию работ по защите информации ОАО «НЗГА» осуществляет директор.

7.16. Руководство и организацию работ по защите информации ОАО «НЗГА» осуществляет заместитель директора курирующий вопросы безопасности, режима и кадров.

7.17. Проведение работ по защите информации ОАО «НЗГА» осуществляет специалист по защите информации.

8. ОРГАНИЗАЦИОННЫЕ МЕРЫ ДЛЯ ОБЕСПЕЧЕНИЯ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОАО «НЗГА»

8.1. Организационные меры регламентируют процессы функционирования ИС, использование его ресурсов, деятельность персонала, а также порядок взаимодействия пользователей для исключения возможностей реализации угроз ИБ и снижения размера потерь в случае их реализации.

8.2. К организационным мерам по защите информации в ИС относятся:

обеспечение особого режима допуска на территорию (в помещение), где может быть осуществлён доступ к информации, циркулирующей в ИС (материальным носителям информации);

разграничение доступа к информации по кругу лиц и характеру информации;

организация и обеспечение работы веб-ресурса и электронной почты.

8.3. Обеспечение особого режима допуска на территорию (в помещение), где может быть осуществлён прямой доступ к информации, циркулирующей в ИС (материальным носителям информации), включает:

безопасность оборудования;

регламентацию порядка проведения профилактических, ремонтно-настроечных и аварийно-восстановительных работ на оборудовании.

8.4. Безопасность оборудования компонентов ИС включает:

механические и электромеханические средства защиты помещений, в которых размещается оборудование ИС (механические и электромеханические замки и иные конструкции, создающие реальное физическое препятствие для нарушителя);

систему кондиционирования;

определение перечня лиц, имеющих право доступа к техническим средствам обработки и защиты информации в ИС. Перечень разрабатывается руководителем подразделения, ответственным за эксплуатацию оборудования, и утверждается его непосредственным начальником.

8.5. Организационные меры по разграничению доступа к информации по кругу лиц и характеру работ включают:

создание индивидуальных учетных записей всех пользователей ИС;

назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями;

контроль корректности назначения ролей и прав доступа пользователей ИС;

определение обязанностей и ответственность обслуживающего персонала ИС (осуществляющего управление оборудованием, общесистемным ПО, ПО компонентов ИС, включая средства защиты информации, сопровождение бизнес-процессов и мониторинг ИБ);

обеспечение резервирования и уничтожение информации;

обеспечение антивирусной защиты;

обеспечение учёта и хранение носителей информации, исключающее хищение и подмену.

8.6. Организация и обеспечение работы веб-ресурса и электронной почты ОАО «НЗГА» осуществляется на договорной основе с Операторами облачных технологий и на основании соответствующих правил оказания таких услуг. В рамках таких услуг, Операторы обеспечивают защиту указанных ресурсов путем обеспечения предоставляемой инфраструктуры необходимыми средствами защиты информации в соответствии с утвержденной у Оператора и согласованной с ОАЦ политикой безопасности. Кроме того, в соответствии с правилами оказания услуг, Оператор несет ответственность за работоспособность данных ресурсов и за резервирование информации.

9. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

9.1. ИС ОАО «НЗГА» взаимодействует с ИС сторонних организаций при помощи системы межведомственного электронного документооборота государственных органов Республики Беларусь.

9.2. Взаимодействие с ИС указанными в п. 9.1 осуществляется в порядке, определенном оператором этих ИС – республиканским унитарным предприятием «Национальный центр электронных услуг». Порядок оказания этих услуг опубликован на официальном сайте РУП «НЦЭУ».

9.3. Указанное взаимодействие осуществляется в целях исполнения требований законодательства Республики Беларусь

и предусматривает подключение к различным государственным информационным системам. Кроме того, значительный объем информационного взаимодействия происходит с аффилированными юридическими лицами, включая нерезидентов Республики Беларусь.

9.4. К таким системам относятся:

ИС, используемые иными аффилированными юридическими лицами

Портал Фонда социальной защиты населения (Министерства труда и социальной защиты населения Республики Беларусь);

Портал электронных счетов-фактур (Министерства по налогам и сборам Республики Беларусь).

Портал ГПО «Белтопгаз», для обмена отчетной информацией с вышестоящей организацией, взаимодействие осуществляется при помощи выделенных каналов связи РУП «Белтелеком». Требования к этому взаимодействию определяет вышестоящая организация.

9.5. Для получения справочной и другой информации, необходимой для обеспечения работы специалистов ОАО «НЗГА», организуются подключения ИС к соответствующим информационным поисковым системам (например: ИПС «Стандарт», ИПС «Эталон» и др.). Порядок такого подключения определяется в соответствующих договорах на оказание услуг и используют имеющиеся в ИС ОАО «НЗГА» подключения к сети Интернет.

10. ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ

10.1. Актуализация настоящей Политики проводится по необходимости, но не реже одного раза в год с целью приведения в соответствие защитных мер реальным угрозам и требованиям к защите информации.

10.2. Специалистами, на которых возложены обязанности по защите информации периодически, не реже одного раза в 12 месяцев, проводится анализ состояния безопасности ИС с целью подтверждения пригодности и эффективности действующей Политики.

10.3. При проведении анализа пригодности Политики ИБ ИС рассматриваются следующие вопросы:

выполнение требований Политики ИБ пользователями ИС;

претензии, поступившие от пользователей ИС, администраторов и иных работников в отношении процессов безопасности;

сведения об инцидентах ИБ и принятые действия по их нейтрализации;

состав персонала и необходимость его обучения, повышения квалификации;

актуальность применяемых мер.

10.4. Внеплановая актуализация Политики производится в следующих случаях:

при изменении нормативных правовых актов и (или) документов (инструкций, положений, руководств), касающихся ИБ ИС;

при внесении изменений в средства защиты информации ИС;

при инциденте (инцидентах) ИБ, который создаёт угрозу безопасного функционирования ИС.

11. КОНТРОЛЬ СОБЛЮДЕНИЯ МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ

11.1. Контроль за выполнением мероприятий, предусмотренных Политикой, возлагается на заместителя директора, курирующего вопросы безопасности, режима и кадров Мащара В.А. Реализация мер по защите информации возлагается на специалиста по защите информации.

11.2. Причины нарушения функционирования ИС выясняются в ходе проведения служебного расследования или проверочных мероприятий.

11.3. Для проведения служебного расследования (выяснения причин, обстоятельств происшествия и установления виновных лиц), решением руководства ОАО «НЗГА» назначается комиссия. В состав комиссии в обязательном порядке включается специалист по защиты информации.

11.4. По решению комиссии и (или) руководителя ОАО «НЗГА», пользователь ИС, причастный к нарушению ее работы, сети или ресурса может быть отстранён от доступа к ИС, АРМ и (или) сети, ресурса.

11.5. Служебное расследование проводится в срок до 30 дней в соответствии с порядком, установленным в ОАО «НЗГА». При наличии оснований, срок расследования может быть продлён.

11.6. К лицам, действия которых повлекли уничтожение, блокирование, модификацию, разглашение, несанкционированное копирование информации либо нарушение работы информационных систем, сетей, ресурсов, нанесение материального ущерба ОАО «НЗГА», применяются меры в соответствии с действующим законодательством.

11.7. После устранения последствий инцидента информационной безопасности и восстановления штатного функционирования систем проводятся мероприятия по предотвращению повторного возникновения инцидента.

11.8. Администратор ИС или другой персонал, обслуживающий ИС, несут ответственность за обеспечение функционирования системы защиты информации в рамках своей должностной инструкции.

11.9. Факт ознакомления и выполнения требований настоящей Политики ИБ ИС закрепляется личной подписью в листе ознакомления, оформленному согласно приложению.