ГЛАВА
РЕСПУБЛИКИ САХА (ЯКУТИЯ)

САХА ӨРӨСПҮҮБҮЛҮКЭТИН
ИЛ ДАРХАНА

УКАЗ

ЫЙААХ

г. Якутск

Дьокуускай к.

О внесении изменений в Указ Главы Республики Саха (Якутия) от 26 марта 2018 г. № 2476 «Об утверждении порядка обеспечения защиты информации в органах государственной власти Республики Саха (Якутия)»

В целях реализации Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», повышения уровня информационной безопасности п о с т а н о в л я ю:

1. Внести в Указ Главы Республики Саха (Якутия) от 26 марта 2018 г. № 2476 «Об утверждении порядка обеспечения защиты информации в органах государственной власти Республики Саха (Якутия)» следующие изменения:

1) пункт 1 изложить в следующей редакции:

«1. Утвердить:

1) порядок обеспечения защиты информации в органах государственной власти Республики Саха (Якутия) согласно приложению № 1 к настоящему Указу;

2) политику информационной безопасности в органах государственной власти Республики Саха (Якутия) согласно приложению № 2 к настоящему Указу;

3) перечень недопустимых событий от реализации угроз безопасности информации, обрабатываемой в ресурсах и сервисах органов государственной власти Республики Саха (Якутия), а также негативных последствий, которые могут быть результатом реализации угроз, согласно приложению № 3 к настоящему Указу.»;

2) пункт 2 изложить в следующей редакции:

«2. Возложить:

1) полномочия по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты,

определению структурных подразделений по защите информации, а также разработке нормативных правовых актов, устанавливающих порядок обеспечения защиты информации в органах государственной власти Республики Саха (Якутия), на заместителя Председателя Правительства Республики Саха (Якутия) Местникова С.В.;

2) осуществление функций по обеспечению информационной безопасности органов государственной власти Республики Саха (Якутия), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты на Министерство инноваций, цифрового развития и инфокоммуникационных технологий Республики Саха (Якутия);

3) персональную ответственность за обеспечение информационной безопасности соответствующих органов (организаций) на руководителей органов (организаций).»;

3) порядок обеспечения защиты информации в органах государственной власти Республики Саха (Якутия) изложить в редакции согласно приложению № 1 к настоящему Указу;

4) дополнить приложением № 2 «Политика информационной безопасности в органах государственной власти Республики Саха (Якутия)» согласно приложению № 2 к настоящему Указу;

5) дополнить приложением № 3 «Перечень недопустимых событий от реализации угроз безопасности информации, обрабатываемой в ресурсах и сервисах органов государственной власти Республики Саха (Якутия), а также негативных последствий, которые могут быть результатом реализации угроз» согласно приложению № 3 к настоящему Указу.

2. Опубликовать настоящий Указ в официальных средствах массовой информации.

Глава
Республики Саха (Якутия) **А. НИКОЛАЕВ**

21 августа 2023 г.
№ 2951

Приложение № 1

к Указу Главы
Республики Саха (Якутия)
от 21 августа 2023 г. № 2951

ПОРЯДОК
обеспечения защиты информации в органах государственной власти Республики Саха (Якутия)

1. Общие положения

1.1. Настоящий порядок является обязательным для исполнения в органах государственной власти Республики Саха (Якутия) при проведении работ по защите информации ограниченного доступа, в том числе составляющей государственную тайну.

1.2. Информация ограниченного доступа по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и сведения конфиденциального характера.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Отнесение информации к государственной тайне осуществляется в соответствии с Законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне». Перечень сведений, отнесенных к государственной тайне, определяется статьей 5 указанного закона.

Перечень сведений конфиденциального характера утвержден Указом Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

1.3. Настоящий порядок определяет структуру системы защиты информации Республики Саха (Якутия), ее задачи и функции, основы организации защиты информации ограниченного доступа, в том числе сведений, содержащих государственную тайну.

1.4. Работа по защите информации в органах государственной власти Республики Саха (Якутия) выполняется на основе законодательных актов Российской Федерации.

1.5. Защита информации осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам и предотвращению несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения путем проведения специальных работ, порядок организации и выполнения которых определяет Совет Безопасности Российской Федерации.

1.6. Главными направлениями работ по обеспечению защиты информации являются:

1) обеспечение эффективного управления системой защиты информации;

2) определение сведений, охраняемых от технических средств разведки;

3) разработка организационно-технических мероприятий по защите информации и их реализация;

4) анализ и оценка реальной опасности перехвата информации, несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в технических средствах, выявление возможных технических каналов утечки информации, подлежащих защите;

5) организация и проведение контроля состояния защиты информации.

1.7. Основными организационно-техническими мероприятиями по защите информации являются:

1) аттестация объектов, обрабатывающих информацию ограниченного доступа, не содержащую сведения, составляющие государственную тайну;

2) аттестация объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;

3) сертификация средств защиты информации и контроль за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам;

4) создание и применение информационных и автоматизированных систем управления в защищенном исполнении;

5) внедрение технических решений и элементов защиты информации при создании и эксплуатации объектов, систем и средств информатизации и связи;

6) использование средств защиты информации (специального и общего применения) и контроль за их эффективностью;

7) применение специальных методов, технических мер и средств защиты информации, исключающих перехват информации, передаваемой по каналам связи.

1.8. Проведение любых мероприятий и работ с использованием информации ограниченного доступа, в том числе составляющей государственную тайну, без принятия необходимых мер по их защите не допускается.

2. Цели и задачи обеспечения защиты информации

2.1. Целями обеспечения защиты информации являются:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализация прав на доступ к информации.

2.2. Основными задачами обеспечения защиты информации являются:

1) проведение единой технической политики, организация и координация работ по защите информации;

2) исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе ее обработки, передачи и хранения;

3) принятие в пределах компетенции нормативно-правовых актов, регулирующих отношения в области защиты информации;

4) организация и создание структурных подразделений, а также выделение штатной единицы специалистов по защите информации;

5) контроль обеспечения защиты информации.

3. Структура системы защиты информации в Республике Саха (Якутия)

3.1. Систему защиты информации в Республике Саха (Якутия) образуют:

1) Совет по информационной безопасности при Главе Республики Саха (Якутия);

2) Министерство инноваций, цифрового развития и инфокоммуникационных технологий Республики Саха (Якутия);

3) руководители органов государственной власти Республики Саха (Якутия);

4) специалисты (структурные подразделения), ответственные за обеспечение защиты информации;

5) постоянно действующие технические комиссии органов государственной власти Республики Саха (Якутия) по защите государственной тайны и (или) конфиденциальной информации;

6) лицензиаты в области защиты информации.

3.2. Совет по информационной безопасности при Главе Республики Саха (Якутия):

1) возглавляет систему обеспечения защиты информации в Республике Саха (Якутия);

2) проверяет и оценивает состояние системы обеспечения защиты информации в органах государственной власти Республики Саха (Якутия) и оказывает методическую помощь в организации и проведении мероприятий по защите информации;

3) проводит работы в соответствии с Положением о Совете по информационной безопасности при Главе Республики Саха (Якутия).

3.3. Министерство инноваций, цифрового развития и инфокоммуникационных технологий Республики Саха (Якутия) является ответственным исполнительным органом государственной власти Республики Саха (Якутия) за обеспечение защиты информации в органах государственной власти Республики Саха (Якутия), координацию деятельности указанных органов по защите информации, обеспечению контроля за состоянием системы защиты информации в Республике Саха (Якутия) и проведению единой политики в области защиты информации в органах государственной власти Республики Саха (Якутия).

3.4. Руководители органов государственной власти Республики Саха (Якутия):

1) осуществляют координацию и руководство по защите информации в подведомственных органам государственной власти Республики Саха (Якутия) организациях (предприятиях);

2) проводят техническую политику, организовывают, обеспечивают и контролируют деятельность соответствующего органа государственной власти Республики Саха (Якутия) и подведомственных ему организаций по вопросам обеспечения защиты информации;

3) вносят предложения по организации защиты информации в Совет по информационной безопасности при Главе Республики Саха (Якутия);

4) несут персональную ответственность за обеспечение защиты информации в соответствующих органах государственной власти Республики Саха (Якутия).

3.5. Структурные подразделения (специалисты) по защите информации непосредственно выполняют функции по обеспечению защиты информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну, в соответствии с федеральным и республиканским законодательством, правовыми актами Федеральной службы безопасности России и Федеральной службы по техническому и экспортному контролю России.

3.6. Постоянно действующие технические комиссии органов государственной власти Республики Саха (Якутия) по защите государственной тайны и (или) информации конфиденциального характера обеспечивают коллегиальное управление системой защиты информации, организацию и координацию работ по противодействию нарушения целостности, доступности и конфиденциальности информации ограниченного доступа.

3.7. Лицензиаты в области защиты информации оказывают услуги и (или) выполняют работу на основании соответствующей лицензии Федеральной службы безопасности России и Федеральной службы по техническому и экспортному контролю России.

4. Организация обеспечения защиты информации

4.1. Защита информации в органах государственной власти Республики Саха (Якутия) является составной частью работ при создании и эксплуатации информационных систем, ресурсов и осуществляется во всех органах государственной власти Республики Саха (Якутия).

4.2. Работы по обеспечению защиты информации в органах государственной власти Республики Саха (Якутия) включаются в ежегодные планы организационно-технических мероприятий. Результаты работ рассматриваются на итоговых отчетах соответствующих постоянно действующих технических комиссий органов государственной власти Республики Саха (Якутия).

4.3. По итогам очередного года результаты работ постоянно действующих технических комиссий органов государственной власти Республики Саха (Якутия) представляются в Совет по информационной безопасности при Главе Республики Саха (Якутия).

4.4. Деятельность по обеспечению защиты информации в органах государственной власти Республики Саха (Якутия) включает:

1) работы по предотвращению специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации, достигаемому с применением специальных программных и аппаратных средств защиты (антивирусные процессоры, программы), организацией системы контроля безопасности программного обеспечения;

2) работы по предотвращению утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований, достигаемому посредством применения защищенных технических средств, аппаратных средств защиты, экранирования зданий или отдельных помещений, контролируемой зоны вокруг средств информатизации, с использованием других организационных и технических мер;

3) работы по исключению несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации, достигаемому посредством применения специальных программно-технических средств защиты, использования криптографических способов защиты, иных организационных и режимных мероприятий;

4) работы по выявлению внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств), достигаемому путем проведения специальных проверок по выявлению этих устройств.

4.5. Информация ограниченного доступа должна обрабатываться с использованием технических и программных средств защиты, сертифицированных в установленном порядке.

4.6. Соответствие технического средства и его программного обеспечения требованиям защищенности подтверждается сертификатом, выдаваемым предприятием, имеющим лицензию на этот вид деятельности, по результатам сертификационных испытаний или предписанием на эксплуатацию, оформляемым по результатам специальных исследований и специальных проверок технических средств и программного обеспечения.

4.7. Для оценки готовности систем проводится аттестация указанных систем и средств в реальных условиях эксплуатации на предмет соответствия принимаемых методов, мер и средств защиты требуемому уровню безопасности информации.

5. Контроль за состоянием обеспечения защиты информации

5.1. Контроль за состоянием обеспечения защиты информации в органах государственной власти Республики Саха (Якутия) заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты информации, решений Совета Безопасности Российской Федерации, нормативно-правовых актов Федеральной службы по техническому и экспортному контролю России, решений межведомственной комиссии полномочного представителя Президента Российской Федерации в Дальневосточном федеральном округе по информационной безопасности, решений Совета по информационной безопасности при Главе Республики Саха (Якутия), поручений Министерства инноваций, цифрового развития и инфокоммуникационных технологий Республики Саха (Якутия), а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения выполнения утвержденных требований и норм по защите информации.

5.2. Контроль осуществляется по решению Совета по информационной безопасности при Главе Республики Саха (Якутия) или Министерства инноваций, цифрового развития и инфокоммуникационных технологий Республики Саха (Якутия) структурными подразделениями (специалистами) органов государственной власти Республики Саха (Якутия), входящими в государственную систему защиты информации, и предприятиями (организациями) в соответствии с их компетенцией.

5.3. Органы государственный власти Республики Саха (Якутия) организуют и осуществляют контроль за подведомственными им организациями через свои подразделения (специалистов) по защите информации.

5.4. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам. Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

5.5. Нарушения по степени важности делятся на три категории:

1) нарушение 1 категории – невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки по техническим каналам;

2) нарушение 2 категории – невыполнение требований по защите информации, в результате чего создаются предпосылки к ее утечке по техническим каналам;

3) нарушение 3 категории – невыполнение других требований по защите информации.

5.6. При обнаружении нарушений первой категории руководители органов государственной власти Республики Саха (Якутия) обязаны:

1) немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения, и принять меры по их устранению;

2) организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц;

3) уведомить Министерство инноваций, цифрового развития и инфокоммуникационных технологий Республики Саха (Якутия), Управление ФСТЭК России по Дальневосточному федеральному округу, Управление ФСБ России по Республике Саха (Якутия) о вскрытых нарушениях и принятых мерах.

5.7. Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер.

5.8. При обнаружении нарушений второй и третьей категории руководители органов государственной власти Республики Саха (Якутия) обязаны принять необходимые меры по их устранению в сроки, согласованные с органом, проводившим проверку.

5.9. По результатам проверок вносятся предложения о применении мер дисциплинарного характера в отношении виновных лиц в адрес Главы Республики Саха (Якутия).

5.10. Допуск представителей Управления ФСТЭК России по Дальневосточному федеральному округу, Управления ФСБ России по Республике Саха (Якутия), структурных подразделений органов государственной власти Республики Саха (Якутия) по защите информации, органа аттестации на объекты для проведения контроля за состоянием защиты информации, к работам и документам, необходимым для проведения контроля, осуществляется в установленном порядке по предъявлении специального удостоверения и предписания на право проведения проверки данного объекта.

6. Финансирование мероприятий по обеспечению защиты информации

6.1. Финансирование мероприятий по защите информации ограниченного доступа, в том числе содержащей сведения, составляющие государственную тайну, в органах государственной власти Республики Саха (Якутия) осуществляется за счет средств государственного бюджета Республики Саха (Якутия).

6.2. Средства на финансирование мероприятий по защите информации ограниченного доступа, в том числе содержащей сведения, составляющие

государственную тайну, в органах государственной власти Республики Саха (Якутия) предусматриваются в государственной программе Республики Саха (Якутия) «Инновационное и цифровое развитие в Республике Саха (Якутия)».

Приложение № 2

к Указу Главы
Республики Саха (Якутия)
от 21 августа 2023 г. № 2951

ПОЛИТИКА
информационной безопасности в органах государственной власти Республики Саха (Якутия)

Определения

Защита информации	–	деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
Информация	–	сведения (сообщения, данные) независимо от формы их представления
Информация ограниченного доступа	–	информация, доступ к которой ограничен федеральными законами
Информационная система	–	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Конфиденциальность информации	–	обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
Обладатель информации	–	лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам
Персональные данные	–	любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)

Обозначения и сокращения

Конфиденциальная информация	–	КИ
Межсетевой экран	–	МЭ
Несанкционированный доступ	–	НСД
Система защиты информации	–	СЗИ
Средство криптографической защиты информации	–	СКЗИ
Средство защиты информации	–	СрЗИ
Федеральная служба безопасности Российской Федерации	–	ФСБ России
Федеральная служба по техническому и экспортному контролю	–	ФСТЭК России

1. Общие положения

1.1. Настоящая политика является документом, доступным всем сотрудникам органов государственной власти Республики Саха (Якутия) (далее – ОГВ РС(Я)) и всем пользователям их ресурсов, и представляет собой официально принятую систему взглядов на обеспечение информационной безопасности в ОГВ РС(Я).

1.2. Основной задачей в области информационной безопасности признается совершенствование мер и средств обеспечения информационной безопасности информационных ресурсов Республики Саха (Якутия) в контексте развития законодательства и норм регулирования информационной деятельности.

1.3. В рамках своей деятельности сотрудники ОГВ РС(Я) обязуются предпринимать все возможные меры для защиты информации от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности или других противоправных действий, связанных с нарушением информационной безопасности.

1.4. Требования информационной безопасности, которые предъявляются к сотрудникам ОГВ РС(Я), соответствуют целям деятельности ОГВ РС(Я) и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.5. Реализация и контроль исполнения требований, установленных настоящей политикой, осуществляется работниками структурных подразделений ОГВ РС(Я), ответственных за информационную безопасность,

в соответствии со своими должностными инструкциями и другими внутренними документами ОГВ РС(Я) по информационной безопасности.

2. Цели и задачи обеспечения информационной безопасности

2.1. Целями обеспечения информационной безопасности ОГВ РС(Я) являются:

1) защита интересов ОГВ РС(Я) от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем Республики Саха (Якутия), нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;

2) обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов и предоставляемых сервисов;

3) соблюдение правового режима использования массивов и программ обработки информации;

4) предотвращение реализации угроз безопасности для деятельности ОГВ РС(Я).

2.2. Объектами информационных правоотношений являются:

1) информационные ресурсы, в том числе с ограниченным доступом;

2) процессы обработки информации в информационных системах ОГВ РС(Я), информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

3) информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации;

4) системы и средства защиты информации, объекты и помещения, в которых размещены хранилища информации.

2.3. Субъектами информационных отношений при использовании информационных систем ОГВ РС(Я), заинтересованными в обеспечении информационной безопасности, являются:

1) ОГВ РС(Я) как собственник информационных ресурсов;

2) работники подразделений ОГВ РС(Я) как пользователи и поставщики информации в информационные системы;

3) юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах ОГВ РС(Я).

2.4. Субъекты информационных отношений заинтересованы в обеспечении:

конфиденциальности определенной части информации;

целостности информации;

своевременного доступа к необходимой им информации;

защиты от навязывания им ложной (недостоверной, искаженной) информации;

разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

защиты соответствующей части информации от незаконного ее тиражирования и распространения.

2.5. Для достижения целей защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности ОГВ РС(Я) должна обеспечивать решение следующих задач:

1) защита от вмешательства в процесс функционирования информационных систем посторонних лиц (возможность использования системы и доступ к ее ресурсам должны иметь только зарегистрированные пользователи);

2) разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационных систем (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей);

3) регистрация и периодический контроль действий пользователей при использовании защищаемых ресурсов и периодический контроль корректности их действий;

4) контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

5) защита от несанкционированной модификации и контроль целостности используемых в ОГВ РС(Я) программных средств и данных, а также защита от несанкционированного внедрения вредоносных программ;

6) защита информации ограниченного доступа, хранимой, обрабатываемой в ОГВ РС(Я), от несанкционированного разглашения или искажения;

7) обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и

получателя информации), а также определение автора при создании и модификации информации;

8) обеспечение исправности применяемых в информационных системах ОГВ РС(Я) средств защиты информации;

9) своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации;

10) создание условий для минимизации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации в ОГВ РС(Я).

2.6. Решение вышеперечисленных задач в ОГВ РС(Я) осуществляется путем:

1) учета всех подлежащих защите информационных ресурсов (каналов связи, аппаратных и программных средств);

2) регламентации процессов обработки подлежащей защите информации, действий работников ОГВ РС(Я) и персонала, осуществляющего обслуживание и модификацию программных и технических средств, на основе утвержденных организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

3) назначения и подготовки работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в ОГВ РС(Я);

4) наделения каждого работника минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам;

5) знания и строгого соблюдения всеми работниками, использующими и обслуживающими аппаратные и программные средства, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

6) персональной ответственности за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам информационных систем;

7) реализации технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных;

8) принятия мер по обеспечению физической целостности технических средств информационных систем и поддержанию необходимого уровня защищенности их компонентов;

9) использования физических и технических (программно-аппаратных) средств защиты ресурсов ОГВ РС(Я) и административной поддержки их использования;

10) контроля соблюдения пользователями информационных систем требований по обеспечению информационной безопасности;

11) юридической защиты интересов ОГВ РС(Я) при взаимодействии с юридическими и физическими лицами от противоправных и несанкционированных действий со стороны этих лиц;

12) проведения анализа эффективности принятых мер и применяемых средств защиты информации в ОГВ РС(Я), разработки и реализации предложений по совершенствованию СЗИ в ОГВ РС(Я).

3. Принципы обеспечения информационной безопасности

3.1. Принцип законности:

1) при выборе защитных мероприятий, реализуемых системой обеспечения информационной безопасности, должно соблюдаться действующее законодательство;

2) принятые меры защиты не должны препятствовать доступу к защищаемой информации со стороны государственных или правоохранительных органов, если такой доступ необходим в случаях, предусмотренных законодательством;

3) программно-технические средства, применяемые в ОГВ РС(Я), должны иметь соответствующие лицензии, официально приобретаться ОГВ РС(Я) у представителей разработчиков этих средств.

3.2. Принцип системности:

1) при построении системы обеспечения информационной безопасности необходимо применять системный подход, который предполагает взаимосвязь процессов организации защиты информационных ресурсов ОГВ РС(Я), согласованное применение методов и средств защиты информационных ресурсов ОГВ РС(Я).

3.3. Принцип координации:

1) при организации действий по обеспечению информационной безопасности руководство ОГВ РС(Я) обеспечивает четкую взаимосвязь соответствующих структурных подразделений между собой, с представителями сторонних организаций, оказывающих услуги в рамках договорных обязательств;

2) при построении, внедрении и эксплуатации системы обеспечения информационной безопасности руководство ОГВ РС(Я) обеспечивает условия

для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

3.4. Принцип дружественности и простоты:

1) система обеспечения информационной безопасности в ОГВ РС(Я) формируется таким образом, чтобы сделать максимально прозрачными для пользователей информационных систем ОГВ РС(Я) процессы ее функционирования;

2) система обеспечения информационной безопасности в ОГВ РС(Я) выстраивается таким образом, чтобы ограничения организационного и технического характера, налагаемые на сотрудников ОГВ РС(Я) в связи с реализацией защитных мер, существенно не затрудняли работу с ресурсами информационных систем ОГВ РС(Я).

3.5. Принцип превентивности:

1) меры, применяемые ОГВ РС(Я) с целью обеспечения информационной безопасности, должны носить упреждающий характер и не допускать реализацию соответствующих угроз и атак.

3.6. Принцип оптимальности и многоуровневости:

1) выбор единых программно-технических средств с целью сокращения расходов на создание и поддержку функционирования компонентов системы обеспечения информационной безопасности;

2) применение разнородных программно-технических средств защиты с целью построения целостной системы обеспечения информационной безопасности и устранения возможных уязвимостей;

3) использование для создания разных рубежей обеспечения информационной безопасности средств, которые имеют схожие друг с другом функции, но разработанные различными производителями и имеющие различную логику построения защитных механизмов.

3.7. Принцип экономической целесообразности:

1) осуществление оценки уровня затрат на обеспечение безопасности, ценности информационных ресурсов и величины возможного ущерба для ОГВ РС(Я) в случае нарушения конфиденциальности, целостности и доступности информационных ресурсов;

2) выбор необходимого и достаточного уровня защиты информационных ресурсов, при котором затраты, риск и размер возможного ущерба являются приемлемыми.

3.8. Принцип непрерывности и недопустимости открытого состояния:

1) система обеспечения информационной безопасности в ОГВ РС(Я) строится таким образом, чтобы процесс защиты информационных систем ОГВ

РС(Я) осуществлялся непрерывно и целенаправленно на протяжении всего жизненного цикла информационных систем;

2) система обеспечения информационной безопасности в ОГВ РС(Я) при любых возникающих обстоятельствах либо полностью выполняет свои функции, либо полностью блокирует доступ.

3.9. Принцип профессионализма:

1) привлечение для разработки и внедрения системы обеспечения информационной безопасности при необходимости специализированных организаций, наиболее подготовленных к конкретному виду деятельности и имеющих соответствующие лицензии на выполнения работ и практический опыт в данной области;

2) организация профессиональной подготовки своих работников для эксплуатации компонентов системы обеспечения информационной безопасности.

3.10. Принцип выбора решений защиты:

1) ориентация на применение современных высокотехнологичных решений и программно-технических средств защиты, хорошо зарекомендовавших себя, интуитивно понятных и не сложных в эксплуатации;

2) использование оценки степени корректности функционирования и исполнения защитных функций, отказоустойчивости, проверки согласованности конфигурации различных компонентов и возможности осуществления централизованного администрирования при выборе решений по защите информационных систем.

3.11. Принцип развития:

1) развитие и обновление на регулярной основе существующей системы обеспечения информационной безопасности;

2) ориентация на преемственность принятых ранее решений по защите, анализ функционирования информационных систем и самой системы обеспечения информационной безопасности.

3.12. Принцип персональной ответственности и разделения обязанностей:

1) руководство ОГВ РС(Я) определяет права и ответственность конкретного работника (в пределах его должностных обязанностей) за обеспечение безопасности информационных ресурсов ОГВ РС(Я);

2) система обеспечения информационной безопасности ОГВ РС(Я) обеспечивает разделение полномочий в информационных системах, обязанностей и ответственности между работниками, исключающее

возможность нарушения критически важных для ОГВ РС(Я) процессов или создания уязвимостей в защите информационных ресурсов.

3.13. Принцип минимизации привилегий пользователей:

1) обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих функций в ОГВ РС(Я) в соответствии со своими должностными обязанностями.

4. Зоны ответственности участников процесса обеспечения информационной безопасности

4.1. Руководство ОГВ РС(Я):

1) создает условия, при которых каждый работник ОГВ РС(Я) знает свои обязанности и задачи в отношении информационных ресурсов и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликта интересов;

2) назначает работников, ответственных за создание и использование СЗИ, информации, обрабатываемой в ОГВ РС(Я), реализацию процессов обеспечения информационной безопасности, а также их контроля;

3) обеспечивает достаточную численность и квалификацию персонала, ответственного за построение и поддержание процессов обеспечения информационной безопасности, внедрение и управление СЗИ, а также контроль и мониторинг текущего состояния системы обеспечения информационной безопасности ОГВ РС(Я);

4) инициирует, осуществляет поддержку и контролирует выполнение всех процессов обеспечения информационной безопасности в ОГВ РС(Я);

5) анализирует результаты работ по обеспечению информационной безопасности и на их основе принимает решения о необходимости развития системы обеспечения информационной безопасности, ее развитии, возможности принятия остаточных рисков информационной безопасности, выделении ресурсов, необходимых для реализации политики информационной безопасности.

4.2. Компетентные подразделения ОГВ РС(Я):

1) подготавливают предложения по доработке политики информационной безопасности в части технического обеспечения информационных систем ОГВ РС(Я);

2) разрабатывают процедуры эффективного управления техническими и программными средствами информационных систем и применяют их в

практической деятельности в отношении всех систем, действующих в ОГВ РС(Я);

3) организуют проведение необходимого инструктажа работников структурных подразделений в части вопросов безопасной эксплуатации информационных систем;

4) обеспечивают защиту доступа ко всему серверному и коммутационному оборудованию, носителям информации, которые используются в соответствующих структурных подразделениях;

5) осуществляют мероприятия по поддержке сопровождения и использования информационных систем;

6) обеспечивают отказоустойчивость всего программно-аппаратного комплекса и процедуру регламентированного восстановления работоспособности после отказов компонентов;

7) регулярно обновляют программные и программно-аппаратные комплексы СЗИ в ОГВ РС(Я);

8) осуществляют поддержку функционирования информационных систем и принимают необходимые меры по конфигурированию систем для обеспечения необходимого уровня информационной безопасности ОГВ РС(Я);

9) контролируют работоспособность устройств бесперебойного питания критичных для ОГВ РС(Я) информационных систем;

10) обеспечивают физическую защиту помещений, в которых располагаются критичные для ОГВ РС(Я) информационные системы;

11) обеспечивают сопровождение устройств контроля доступа в помещения ОГВ РС(Я);

12) обеспечивают защиту информационных ресурсов ОГВ РС(Я) от случайного или намеренного уничтожения, искажения, разглашения;

13) контролируют выполнение установленных правил и процедур обеспечения информационной безопасности в ОГВ РС(Я).

4.3. Руководители структурных подразделений ОГВ РС(Я);

1) обязаны соблюдать требования действующего законодательства Российской Федерации и внутренних документов ОГВ РС(Я) в части обеспечения информационной безопасности;

2) обеспечивают контроль за соблюдением норм и правил обеспечения информационной безопасности в своем структурном подразделении и информируют компетентное подразделение о любых подозрительных событиях или нарушениях действующих правил обеспечения информационной безопасности;

3) обеспечивают соответствие действий работников подразделения политике информационной безопасности, внутренним документам по

информационной безопасности и любым другим распоряжениям руководства ОГВ РС(Я) по вопросам информационной безопасности;

4) организуют проведение необходимого инструктажа по вопросам выполнения правил информационной безопасности для всех работников своего структурного подразделения;

5) контролируют выполнение работниками в своем структурном подразделении установленных правил в целях обеспечения физической безопасности компьютерного оборудования и носителей информации;

6) своевременно информируют руководство о всех выявленных сбоях в работе информационных систем;

7) контролируют доступ к необходимым информационными ресурсам работников своего структурного подразделения в соответствии с потребностью в пределах служебных обязанностей.

4.4. Работники ОГВ РС(Я):

1) соблюдают и выполняют требования политики информационной безопасности, соответствующих локальных актов, документов ОГВ РС(Я) по вопросам информационной безопасности;

2) соблюдают конфиденциальность данных, доступ к которым был ими получен;

3) обеспечивают физическую безопасность всего технического оборудования и носителей информации, используемых в работе;

4) не допускают самовольного подключения и использования в автоматизированной информационной системе личного компьютерного и цифрового оборудования, а также носителей информации;

5) не допускают самовольную установку программного обеспечения на компьютеры, входящие в состав информационной системы;

6) своевременно информируют руководителя своего структурного подразделения о всех случаях нарушения информационной безопасности и о всех выявленных сбоях в работе программных и программно-аппаратных средств;

7) проявляют осмотрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности.

4.5. Сторонние физические и юридические лица соблюдают и выполняют требования политики информационной безопасности, соответствующих локальных актов и документов ОГВ РС(Я) и других распоряжений руководства по вопросам информационной безопасности при исполнении договорных обязательств.

5. Основные требования по защите информации ограниченного доступа

5.1. Общие требования:

1) в ОГВ РС(Я) необходимо соблюдать режим безопасности, предусматривающий реализацию организационно-технических мероприятий, направленных на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с требованиями законодательства Российской Федерации;

2) в ОГВ РС(Я) осуществляется обработка и хранение информации ограниченного доступа (доступ к которой ограничен федеральными законами и служебной необходимостью);

3) в ОГВ РС(Я) должен быть разработан перечень информации ограниченного доступа;

4) орган, как обладатель информации ограниченного доступа, при осуществлении своих прав обязан:

соблюдать права и законные интересы иных лиц;

принимать меры по защите информации;

ограничивать доступ к информации, если такая обязанность установлена федеральными законами;

5) орган, как обладатель информации ограниченного доступа, если иное не предусмотрено федеральными законами, вправе:

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 законом основании;

защищать установленными законом 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 регуляторов;

6) орган, являясь обладателем информации ограниченного доступа, в случаях, установленных законодательством РФ, обязан обеспечить:

предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

своевременное обнаружение фактов несанкционированного доступа к информации;

недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

возможность регламентированного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением уровня защищенности информации;

7) защита информации ограниченного доступа представляет собой принятие правовых, 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).

5.2. Организация защиты конфиденциальной информации:

1) при организации в ОГВ РС(Я) защиты информации ограниченного доступа необходимо руководствоваться требованиями федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации;

2) в ОГВ РС(Я) необходимо соблюдать режим защиты конфиденциальной информации (далее – КИ):

ограничение доступа к КИ путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;

регулирование отношений по использованию КИ с работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

использование материальных носителей, содержащих КИ, в соответствии с утвержденным порядком, исключающим несанкционированный доступ к ним;

3) для обеспечения защиты КИ орган вправе применять средства и методы технической защиты, предпринимать другие не противоречащие законодательству РФ меры;

4) в целях охраны КИ в рамках трудовых отношений необходимо:

ознакомить под расписку работников, доступ которых к КИ необходим для выполнения ими своих служебных обязанностей, с перечнем КИ и установленным в ОГВ РС(Я) режимом защиты КИ, а также мерами ответственности за его нарушение;

создать работникам необходимые условия для соблюдения установленного режима защиты КИ;

5) работники ОГВ РС(Я) обязаны выполнять установленный в ОГВ РС(Я) режим защиты КИ, не разглашать информацию, составляющую КИ, и не использовать эту информацию в личных целях.

5.3. Особенности защиты персональных данных:

1) при организации в ОГВ РС(Я) защиты персональных данных необходимо руководствоваться требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», который регулирует отношения, связанные с обработкой и хранением персональных данных граждан и определяет требования по защите их конфиденциальности;

2) ОГВ РС(Я) 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;

3) перечень мер, выполнение которых обеспечивает ОГВ РС(Я) в качестве оператора персональных данных, должен включать:

назначение в ОГВ РС(Я) ответственного за организацию обработки персональных данных;

издание ОГВ РС(Я) 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;

применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ;

оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

ознакомление работников ОГВ РС(Я), непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику ОГВ РС(Я) в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и обучение, при необходимости, указанных работников;

4) ОГВ РС(Я) при обработке персональных данных обязан 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) обеспечение безопасности персональных данных достигается в частности:

определением угроз и нарушителей безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн);

проведением классификации ИСПДн в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и определением класса защищенности для ИСПДн;

применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает выбранные уровни защищенности персональных данных;

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

оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

учетом машинных носителей персональных данных;

обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

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

контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн;

6) работники ОГВ РС(Я) должны быть ознакомлены под подпись с документами ОГВ РС(Я), устанавливающими порядок обработки персональных данных, а также об их правах, обязанностях и ответственности.

6. Основные требования к процессам обеспечения информационной безопасности

6.1. Общие положения:

1) методическое руководство, разработку конкретных требований по защите информации, согласование выбора средств вычислительной техники и связи, технических и программных средств защиты, организацию работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации осуществляют компетентные подразделения ОГВ РС(Я).

6.2. Физическая безопасность и безопасность на рабочем месте:

1) система защиты зданий и помещений ОГВ РС(Я), объектов и технических средств информационных систем ОГВ РС(Я) обеспечивает выполнение следующих функций:

разграничение доступа работников в помещения ОГВ РС(Я) в соответствии с их полномочиями и функциональными обязанностями;

регистрация фактов входа работников в помещения с повышенными требованиями к режиму их посещения (серверные помещения, архивы и т.д.);

регистрация фактов входа посторонних лиц в здания ОГВ РС(Я);

предотвращение доступа посторонних лиц в помещения, где размещены аппаратные и сетевые ресурсы информационных систем;

разрешительный режим вноса/выноса (ввоза/вывоза) компьютерного оборудования, средств записи и хранения информации;

2) определяется перечень технических средств, находящихся в специальных контролируемых зонах;

3) к техническим средствам, которые выделяются в специальные контролируемые зоны, необходимо отнести следующие группы ресурсов:

основные информационные серверы и средства вычислительной техники, на которых осуществляются обработка и хранение информации ограниченного распространения;

сетевое оборудование и серверы, обеспечивающие работу критических систем;

файловые серверы, на которых хранятся данные, в том числе резервные;

критичные для деятельности ОГВ РС(Я) системы и коммуникационное оборудование, обеспечивающие внешние коммуникации ОГВ РС(Я);

4) контролируемые зоны защищаются соответствующими системами контроля и управления доступом, обеспечивая доступ только авторизованному персоналу;

5) доступ в контролируемые зоны сторонних лиц или представителей других организаций возможен только в сопровождении уполномоченного работника ОГВ РС(Я);

6) размещение и эксплуатация рабочих станций, серверов и сетевого оборудования ОГВ РС(Я) осуществляются в помещениях, оборудованных замками, средствами сигнализации и (при необходимости) постоянно находящихся под охраной или наблюдением;

7) размещение технических средств вывода и отображения информации в помещениях ОГВ РС(Я) производится с учетом исключения возможности визуального просмотра информации посторонними лицами и персоналом, не допущенным к работе с данной информацией;

8) работники ОГВ РС(Я) на момент своего отсутствия на рабочем месте обязаны исключить возможность наличия на рабочем столе документов или носителей с защищаемой информацией;

9) технические средства и оборудование должны размещаться и храниться таким образом, чтобы сократить возможный риск его повреждения и угрозы несанкционированного доступа;

10) помещения ОГВ РС(Я) должны быть оборудованы детекторами огня и дыма, огнетушителями, системами кондиционирования воздуха, средствами охранно-пожарной сигнализации;

11) основное техническое оборудование ОГВ РС(Я) должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам ОГВ РС(Я) в соответствии с рекомендациями производителя;

12) пользователи портативных технических средств не должны оставлять техническое оборудование и носители информации без присмотра;

13) портативные технические средства не должны оставаться за пределами контролируемой зоны ОГВ РС(Я) дольше, чем того требует служебная необходимость.

6.3. Безопасность при работе с носителями информации:

1) в ОГВ РС(Я) 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;

2) работники ОГВ РС(Я) должны использовать электронные носители информации только для выполнения своих служебных обязанностей. Использование электронных носителей информации в ОГВ РС(Я) в иных целях строго запрещено;

3) электронные носители информации в ОГВ РС(Я) должны быть учтены путем присвоения каждому носителю инвентаризационного номера и назначения владельца;

4) электронные носители информации должны храниться в помещениях, исключающих получение к ним несанкционированного доступа, при этом должен быть обеспечен контроль доступа к носителям;

5) для контроля процессов использования и хранения электронных носителей информации должен быть разработан порядок плановой инвентаризации носителей;

6) в случае кражи или потери электронных носителей информации, а также иных инцидентов, которые могут привести к разглашению защищаемой информации, должны проводиться мероприятия по расследованию указанных инцидентов;

7) при снятии электронного носителя информации с эксплуатации все данные, хранящиеся на нем, должны быть гарантированно стерты;

8) при утилизации электронных носителей информации должна быть обеспечена невозможность восстановления записанной на них информации;

9) факт уничтожения информации и утилизации носителя информации фиксируется в соответствии с порядком, установленным в ОГВ РС(Я).

6.4. Техническое обслуживание оборудования:

1) технические средства всех систем ОГВ РС(Я) должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования;

2) ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированным персоналом;

3) техническое обслуживание оборудования и систем сторонними организациями не должно приводить к риску нарушения конфиденциальности защищаемой информации.

6.5. Взаимодействие с третьими лицами:

1) в целях обеспечения информационной безопасности ОГВ РС(Я) при взаимодействии с третьими лицами должны выполняться следующие мероприятия:

заключение соглашения о неразглашении конфиденциальной информации;

контроль за действиями третьих лиц;

в договорах с третьими лицами предусматривать право ОГВ РС(Я) на проведение аудита обеспечения безопасности той информации, которая передается третьим лицам.

6.6. Управление жизненным циклом информационных систем:

1) мероприятия по управлению жизненным циклом автоматизированных информационных систем должны быть направлены на обеспечение информационной безопасности при вводе в действие, эксплуатации, сопровождении и модернизации, выводе из эксплуатации информационных систем, автоматизирующих деятельность ОГВ РС(Я);

2) основой при выборе или разработке информационных систем должны являться технические задания, содержащие требования информационной безопасности для информационных систем;

3) любое планируемое к внедрению изменение информационной системы предварительно должно быть протестировано на совместимость и отсутствие нарушений работоспособности системных компонентов;

4) работы по модернизации автоматизированной информационной системы, в том числе по установке программного обеспечения и обновлений, должны проводиться в нерабочее время или время наименьшей рабочей нагрузки;

5) при выводе из эксплуатации автоматизированных информационных систем должно обеспечиваться гарантированное удаление обрабатываемой и хранимой в них информации с использованием специализированных программных средств или путем физического уничтожения носителей информации;

6) все процедуры обеспечения информационной безопасности, установленные в ОГВ РС(Я) в отношении информационных систем, должны выполняться и контролироваться ответственными за информационную безопасность лицами.

6.7. Контроль доступа к информационным системам:

1) все работники ОГВ РС(Я), допущенные к работе с информационными системами, несут персональную ответственность за нарушения установленного порядка обработки информации, правил хранения,

использования и передачи находящихся в их распоряжении защищаемых ресурсов системы;

2) уровень полномочий пользователя в информационной системе ОГВ РС(Я) должен определяться в соответствии с его должностными обязанностями и производственной необходимостью;

3) доступ пользователей к информационным системам ОГВ РС(Я) должен контролироваться администратором системы;

4) осуществление регулярного контроля выполнения политик и иных документов, касающихся регламентации допуска работников ОГВ РС(Я) к информационным системам.

6.8. Идентификация и аутентификация:

1) доступ пользователей к информационным системам должен предоставляться только после успешного завершения процедур идентификации, аутентификации и авторизации;

2) получение пользователем имени в системе и парольной информации, которые обеспечивают доступ пользователя к ресурсам системы, должно осуществляться по представлению руководителей структурных подразделений.

6.9. Безопасность пароля:

1) с целью обеспечения защиты от несанкционированного доступа к информационным системам устанавливаются требования к выбору парольной информации, обеспечивающие достаточную степень стойкости паролей;

2) для обеспечения конфиденциальности парольной информации пользователю запрещается хранить значения своих паролей на бумажном носителе в открытом виде и в свободном доступе;

3) для обеспечения конфиденциальности парольной информации пользователям запрещается передавать значения своих паролей третьим лицам;

4) при вводе пароля пользователем для доступа к информационной системе ОГВ РС(Я) должно исключаться отображение парольной информации на экране монитора в открытом виде;

5) процедура смены парольной информации в информационных системах ОГВ РС(Я) должна проводиться на регулярной основе.

6.10. Регистрация событий:

1) осуществление регистрации событий безопасности на всех компонентах информационных систем ОГВ РС(Я), в которых обрабатывается, хранится или посредством которых передается защищаемая информация.

6.11. Использование средств криптографической защиты информации:

1) решение об использовании средств криптографической защиты информации (далее – СКЗИ) в интересах защиты собственных

информационных ресурсов принимается руководством ОГВ РС(Я) в соответствии с законодательством Российской Федерации;

2) при эксплуатации СКЗИ и ключевой информации все сотрудники ОГВ РС(Я) должны выполнять требования нормативных правовых актов, издаваемых федеральным органом исполнительной власти в области обеспечения безопасности, документов ОГВ РС(Я) по обеспечению безопасности использования СКЗИ, а также эксплуатационной документации производителя СКЗИ.

6.12. Безопасность информационной сети:

1) установление надлежащего контроля в отношении локальной вычислительной сети и всех внешних информационных коммуникаций ОГВ РС(Я) для обеспечения защиты данных и защиты информационных систем ОГВ РС(Я) от несанкционированного доступа;

2) должны быть определены цели использования сети Интернет и требования к процедуре использования ресурсов сети Интернет. Использование сети Интернет работников в личных целях должно быть строго запрещено;

3) доступ к информационным сервисам сети Интернет предоставляется работникам ОГВ РС(Я) только в случае производственной необходимости;

4) подключение к сети Интернет должно осуществляться только при организации защиты соединения путем установки МЭ и специальных программных средств защиты;

5) разрешительные политики доступа в Интернет должны технически реализовываться специализированным программным обеспечением;

6) контроль использования работниками ресурсов сети Интернет должен осуществляться уполномоченными работниками на постоянной основе.

6.13. Использование корпоративной электронной почты:

1) система корпоративной электронной почты должна использоваться в ОГВ РС(Я) с целью организации обмена электронными сообщениями между работниками, а также между работниками ОГВ РС(Я) и внешними абонентами;

2) в ОГВ РС(Я) должны быть четко определены требования к использованию системы корпоративной электронной почты;

3) предоставление и прекращение доступа к ресурсам корпоративной электронной почты должны осуществляться только на основе оформленной заявки;

4) в ОГВ РС(Я) должно быть установлено специальное программное обеспечение, осуществляющее контроль всех входящих сообщений на наличие вредоносного программного обеспечения;

5) в ОГВ РС(Я) должны быть предусмотрены механизмы архивирования и резервного копирования корпоративной электронной почты в автоматическом режиме.

6.14. Резервное копирование и восстановление данных:

1) осуществление резервного копирования для:

файловых серверов и серверов приложений, критичных для деятельности ОГВ РС(Я);

операционных систем файловых серверов и прикладных программ;

приложений, критичных для деятельности ОГВ РС(Я);

рабочих данных;

2) частота и режим резервного копирования устанавливаются таким образом, чтобы обеспечить минимальную потерю данных и допустимое время восстановления;

3) резервное копирование и восстановление ресурсов информационных систем должны проводить уполномоченные работники ОГВ РС(Я);

4) резервное копирование должно осуществляться в автоматическом режиме с применением специализированного программно-аппаратного комплекса.

7. Основные требования к процессам управления информационной безопасностью

7.1. Управление рисками:

1) выбор требований по информационной безопасности и защитных механизмов, применяемых в системе информационной безопасности, должен основываться на проведении анализа рисков нарушения основных свойств безопасности для наиболее критичных информационных ресурсов ОГВ РС(Я);

2) основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения свойств целостности, конфиденциальности и доступности для ресурсов информационной системы ОГВ РС(Я);

3) результатом проведения анализа рисков должен быть комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность ОГВ РС(Я) при реализации той или иной угрозы и обеспечивающих достаточный уровень защищенности информационных систем ОГВ РС(Я).

7.2. Управление инцидентами информационной безопасности:

1) для обеспечения эффективного разрешения инцидентов информационной безопасности в ОГВ РС(Я), минимизации потерь и уменьшения риска возникновения повторных инцидентов должно

осуществляться эффективное управление инцидентами информационной безопасности;

2) для управления инцидентами информационной безопасности должна быть создана система учета произошедших инцидентов, которая представляет собой комплекс средств и мероприятий для сбора и консолидации информации об инцидентах;

3) в отношении каждого произошедшего инцидента требуется выполнять анализ и разработку эффективных мер реагирования на данный инцидент;

7.3. Мониторинг текущего уровня информационной безопасности:

1) для обеспечения высокого уровня контроля в отношении системы обеспечения информационной безопасности в ОГВ РС(Я) на постоянной основе должны проводиться комплексный анализ существующих защитных механизмов и возникающих инцидентов информационной безопасности, а также периодический аудит всей системы обеспечения информационной безопасности;

2) процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов;

3) при проведении контрольных мероприятий, связанных с оценкой функционирования защитных мер в ОГВ РС(Я), уполномоченные работники должны придерживаться следующих принципов:

не нарушать функционирование текущей деятельности ОГВ РС(Я);

действовать в соответствии с внутренними документами ОГВ РС(Я) по информационной безопасности;

не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности;

оформлять отчеты, подтверждающие выполнение мероприятий по обеспечению информационной безопасности;

4) информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к функционированию защитных мер, должна консолидироваться и храниться в местах, исключающих получение к ней несанкционированного доступа;

5) мониторинг данных о зарегистрированных событиях информационной безопасности должен проводиться по возможности с использованием встроенных механизмов настройки и аудита событий в

программных и программно-технических средствах, используемых в информационных системах ОГВ РС(Я).

7.4. Аудит системы обеспечения информационной безопасности:

1) в целях оценки текущего уровня информационной безопасности уполномоченные работники ОГВ РС(Я) на регулярной основе должны проводить аудит информационной безопасности;

2) внутренние аудиты или самооценки должны выполняться по возможности работниками ОГВ РС(Я);

3) результатом выполнения аудитов по информационной безопасности должны стать отчеты о выполненном аудите информационной безопасности, которые разрабатываются специалистами ОГВ РС(Я);

4) по результатам аудита уполномоченные работники и ответственные подразделения ОГВ РС(Я) должны определить действия, необходимые для устранения обнаруженных несоответствий в процессе аудита и вызвавших их причин.

7.5. Управление персоналом:

1) организация такого процесса управления персоналом, который обеспечит доверительное отношение к работникам, а также организует комплексное противодействие угрозам информационной безопасности, исходящим от персонала ОГВ РС(Я);

2) выполнение обязательных проверок при приеме новых работников на работу с точки зрения достоверности сообщаемых ими данных и с позиции оценки их профессиональных навыков;

3) организация работы в направлении повышения осведомленности и обучения в области информационной безопасности.

Повышение осведомленности работников ОГВ РС(Я):

по существующим в ОГВ РС(Я) политикам информационной безопасности;

по применяемым в ОГВ РС(Я) защитным мерам;

по правильному использованию защитных мер в соответствии с внутренними документами ОГВ РС(Я).

8. Заключение

8.1. Настоящая политика является общедоступной и подлежит размещению на официальных сайтах ОГВ РС(Я).

8.2. Ответственность должностных лиц ОГВ РС(Я), имеющих доступ к конфиденциальной информации, за невыполнение требований норм, регулирующих обработку и защиту информации, определяется в соответствии

с законодательством Российской Федерации и внутренними документами ОГВ РС(Я).

Приложение № 3

к Указу Главы
Республики Саха (Якутия)
от 21 августа 2023 г. № 2951

ПЕРЕЧЕНЬ
недопустимых событий от реализации угроз безопасности информации, обрабатываемой в ресурсах и сервисах органов государственной власти Республики Саха (Якутия), а также негативных последствий, которые могут быть результатом реализации угроз

Виды риска (ущерба)	Недопустимое событие	Возможные негативные последствия
Ущерб физическому лицу	Разглашение персональных данных	Попадание персональных данных в базы данных мошенников
		Ущерб репутации гражданина
		Получение доступа к личным интернет-ресурсам (социальные сети, личные кабинеты и пр.)
		Ущерб чести и достоинству гражданина
	Финансовый или иной материальный ущерб физическому лицу	Материальный ущерб вследствие разглашения места жительства
		Финансовый ущерб вследствие разглашения личной финансовой информации
Ущерб оператору	Нарушение законодательства РФ в части обеспечения безопасности информации	Административная ответственность за нарушение в области персональных данных
		Административная ответственность за нарушение в области обработки информации в ГИС
	Экономический ущерб в форме штрафов	Штрафы за нарушение правил обработки персональных данных
		Штрафы за нарушение правил обработки информации в ГИС
		Штрафы за неоказание государственных услуг
	Репутационный ущерб	Нарушение деловой репутации, снижение престижа

		Негативные публикации в СМИ
		Публикация в интернет-ресурсах органов власти Республики Саха (Якутия) недостоверной информации
		Дискредитация работников
	Выход из строя технических средств	Выход технических средств из строя вследствие перегрузки вычислительных ресурсов
		Выход технических средств из строя вследствие устаревания и физического износа
		Физический вывод из строя технических средств вследствие действий внутренних нарушителей
Ущерб в социальной сфере	Нарушение выполнения органом власти возложенных на него функций	Снижение эффективности взаимодействия органов власти Республики Саха (Якутия) с населением
		Снижение эффективности взаимодействия органов власти Республики Саха (Якутия) между собой
		Нарушение защищенного электронного документооборота
		Нарушение в работе системы оповещения при чрезвычайных ситуациях
		Нарушение информирования населения о деятельности органов власти
		Нарушение работы системы вызова экстренных служб
	Нарушения предоставления государственных услуг	Нарушение предоставления государственной и муниципальной социальной помощи
		Нарушение работы многофункционального центра предоставления государственных и муниципальных услуг
		Нарушение работы регионального портала государственных и муниципальных услуг
		Нарушения процесса предоставления государственных и муниципальных услуг в электронном виде