ГЛАВА
РЕСПУБЛИКИ САХА (ЯКУТИЯ)

САХА ӨРӨСПҮҮБҮЛҮКЭТИН
ИЛ ДАРХАНА

УКАЗ

ЫЙААХ

г. Якутск

Дьокуускай к.

Об утверждении Порядка обеспечения защиты информации в органах государственной власти Республики Саха (Якутия)

В соответствии с Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05 декабря 2016 г. № 646, в целях установления единой политики в области защиты информации в органах государственной власти Республики Саха (Якутия) п о с т а н о в л я ю:

1. Утвердить прилагаемый Порядок обеспечения защиты информации в органах государственной власти Республики Саха (Якутия).

2. Определить министра связи и информационных технологий Республики Саха (Якутия) лицом, ответственным за обеспечение защиты информации в органах государственной власти Республики Саха (Якутия).

3. Органам государственной власти Республики Саха (Якутия):

3.1. Принять ведомственные правовые акты, регулирующие порядок обеспечения защиты информации.

3.2. Разработать комплекс мер и план мероприятий по защите информации.

3.3. Обеспечить регулярное повышение квалификации специалистов, назначенных во исполнение пункта 1.2 распоряжения Президента Республики Саха (Якутия) от 26 мая 2009 г. № 211-РП «О мерах по защите информации, составляющей государственную тайну, в органах государственной власти и местного самоуправления Республики Саха (Якутия)».

4. Установить персональную ответственность руководителей органов государственной власти Республики Саха (Якутия) за состояние системы

защиты информации в соответствующих органах государственной власти Республики Саха (Якутия).

5. Рекомендовать органам местного самоуправления муниципальных образований Республики Саха (Якутия):

5.1. При обеспечении защиты информации руководствоваться настоящим Указом.

5.2. Принять муниципальные правовые акты, регулирующие порядок обеспечения защиты информации.

5.3. Утвердить муниципальным правовым актом комплекс мер и план мероприятий по защите информации.

5.4. Предусматривать в бюджетах муниципальных образований средства на осуществление мероприятий по защите информации ограниченного доступа.

6. Контроль исполнения настоящего Указа возложить на заместителя Председателя Правительства Республики Саха (Якутия) Никифорова И.Г.

7. Опубликовать настоящий Указ в официальных средствах массовой информации.

Глава
Республики Саха (Якутия) **Е.БОРИСОВ**

26 марта 2018 года

№ 2476

УТВЕРЖДЕН

Указом Главы
Республики Саха (Якутия)
от 26 марта 2018 г. № 2476

П О Р Я Д О К
обеспечения защиты информации в органах государственной власти Республики Саха (Якутия)

I. Общие положения

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 составляющих государственную тайну.

2. 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.

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

4. 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 по безопасности Российской Федерации.

5. Главными направлениями работ по обеспечению защиты информации являются:

обеспечение эффективного управления системой защиты информации;

определение сведений, охраняемых от технических средств разведки;

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

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;

организация и проведение контроля состояния защиты информации.

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

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

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

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

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

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

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

7. 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.

II. Цели и задачи обеспечения защиты информации

8. Целями обеспечения защиты информации являются:

8.1. Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

8.2. Соблюдение конфиденциальности информации ограниченного доступа.

8.3. Реализация прав на доступ к информации.

9. Основными задачами обеспечения защиты информации являются:

9.1. Проведение единой технической политики, организация и координация работ по защите информации.

9.2. 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.

9.3. Принятие в пределах компетенции нормативно-правовых актов, регулирующих отношения в области защиты информации.

9.4. Организация и создание структурных подразделений по защите информации.

9.5. Контроль обеспечения защиты информации.

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

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

Совет информационной безопасности при Главе Республики Саха (Якутия);

министр связи и информационных технологий Республики Саха (Якутия);

руководители органов государственной власти Республики Саха (Якутия);

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

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

лицензиаты в области защиты информации.

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

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

б) 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;

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

12. Министр связи и информационных технологий Республики Саха (Якутия) является ответственным лицом 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).

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

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

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

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

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

14. 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 федеральным и республиканским законодательством, правовыми актами Федеральной службы безопасности России и Федеральной службы по техническому и экспортному контролю России.

15. 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.

16. 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.

IV. Организация обеспечения защиты информации

17. 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).

18. 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).

19. 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).

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

а) 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;

б) 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, экранированием зданий или отдельных помещений, контролируемой зоны вокруг средств информатизации, с использованием других организационных и технических мер;

в) работы по исключению несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации, достигаемому посредством применения специальных программно-технических средств защиты, использованием криптографических способов защиты, иными организационными и режимными мероприятиями;

г) 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.

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

22. 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, оформляемом по результатам специальных исследований и специальных проверок технических средств и программного обеспечения.

23. 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.

V. Контроль за состоянием обеспечения защиты информации

24. 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 по безопасности при Президенте 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 министра связи и информационных технологий Республики Саха (Якутия), а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения выполнения утвержденных требований и норм по защите информации.

25. Контроль проводится по решению Совета по информационной безопасности при Главе Республики Саха (Якутия) или министра связи и информационных 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.

26. Органы государственный власти Республики Саха (Якутия) организуют и осуществляют контроль за подведомственными им

организациями через свои подразделения (специалистов) по защите информации.

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

28. Нарушения по степени важности делятся на три категории:

28.1. Невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность ее утечки по техническим каналам.

28.2. Невыполнение требований по защите информации, в результате чего создаются предпосылки к ее утечке по техническим каналам.

28.3. Невыполнение других требований по защите информации.

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

29.1. Немедленно прекратить работы на участке (рабочем месте), где обнаружены нарушения, и принять меры по их устранению.

29.2. Организовать в установленном порядке расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц.

29.3. Уведомить министра связи и информационных технологий Республики Саха (Якутия), Управление ФСТЭК России по Дальневосточному федеральному округу, Управление ФСБ России по Республике Саха (Якутия) о вскрытых нарушениях и принятых мерах.

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

31. 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.

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

33. 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.

VI. Финансирование мероприятий по обеспечению защиты информации

34. 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).

35. 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) «Развитие информационного общества на 2018 – 2022 годы».