МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ КАМЧАТСКОГО КРАЯ

ПРИКАЗ

11.08.2023 № 137-п

г. Петропавловск-Камчатский

Об утверждении Политики по организации и проведению работ по обеспечению безопасности информации при ее обработке в информационно-телекоммуникационной сети исполнительных органов Камчатского края

ПРИКАЗЫВАЮ:

1. Утвердить Политику по организации и проведению работ по обеспечению безопасности информации при ее обработке в информационно-телекоммуникационной сети исполнительных органов Камчатского края согласно приложению к настоящему приказу.

2. Контроль за исполнением настоящего приказа возложить на Батурина Виталия Александровича, заместителя Министра – начальника отдела инфраструктуры связи Министерства цифрового развития Камчатского края.

И.о. Министра В.А. Батурин

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 44927B7E9FC6135671B8156526444B57
Владелец **Батурин Виталий Александрович**
Действителен с 13.12.2022 по 07.03.2024

Приложение к приказу Министерства
цифрового развития Камчатского края
от 11.08.2023 № 137-п

ПОЛИТИКА
по организации и проведению работ по обеспечению безопасности информации при ее обработке в информационно-телекоммуникационной сети исполнительных органов Камчатского края

1. Общие положения

1. Настоящая Политика по организации и проведению работ по обеспечению безопасности информации при ее обработке в информационно-телекоммуникационной сети исполнительных органов Камчатского края (далее – Политика) определяет мероприятия, процедуры и правила по защите информации в информационно-телекоммуникационной сети исполнительных органов Камчатского края (далее – ИТКС).

2. В настоящей Политике применяются следующие термины и определения:

1) уполномоченный орган иткс – исполнительный орган камчатского края, уполномоченный на координацию деятельности по созданию, развитию, модернизации, эксплуатации ИТКС, регулирование вопросов подключения к ИТКС и вопросов предоставления ресурсов ИТКС, а также вопросов обеспечения информационной безопасности и технической защиты информации в ИТКС;

2) оператор ИТКС – уполномоченная организация, осуществляющая создание, развитие, модернизацию, эксплуатацию ИТКС, обеспечивающая ее устойчивое функционирование, а также информационную безопасность и техническую защиту информации в ИТКС;

3) абонент ИТКС – исполнительный орган Камчатского края, государственный орган Камчатского края, подведомственное им учреждение, иное юридическое лицо, подключенное к ИТКС;

4) ИТКС – информационно-телекоммуникационная сеть, представляющая собой распределенную систему взаимосвязанных персональных компьютеров (рабочих станций), серверов, коммутационного оборудования, структурированной кабельной сети и других средств вычислительной техники;

5) пользователь – работник и (или) лицо, имеющее доступ к информационным, программным и аппаратным ресурсам ИТКС;

6) работник – физическое лицо, вступившее в трудовые отношения с работодателем (Абонентом ИТКС);

7) безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при её обработке в информационной системе;

8) блокирование информации – временное прекращение обработки информации (за исключением случаев, если обработка необходима для уточнения информации);

9) вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению;

10) группа реагирования на инциденты информационной безопасности – группа квалифицированных и доверенных лиц, которая выполняет, координирует и поддерживает реагирование на нарушения информационной безопасности, затрагивающие информационные системы в пределах определённой зоны ответственности;

11) доступ к информации – возможность получения информации и ее использования;

12) доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать;

13) защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

14) идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

15) информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

16) информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

17) информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

18) информация – сведения (сообщения, данные) независимо от формы их представления;

19) конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

20) межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы;

21) нарушитель безопасности информации – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является

нарушение безопасности информации при её обработке техническими средствами в информационной системе;

22) несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами;

23) носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

24) обезличивание – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность данных конкретному субъекту;

25) оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку информации, а также определяющие цели обработки информации, состав информации, подлежащих обработке, действия (операции), совершаемые с информацией;

26) персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

27) правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

28) распространение информации – действия, направленные на раскрытие информации неопределенному кругу лиц;

29) средства криптографической защиты информации – средства шифрования, средства имитозащиты, средства кодирования, средства электронной цифровой подписи, средства изготовления ключевых документов (независимо от вида носителя ключевой информации), ключевые документы (независимо от вида носителя ключевой информации);

30) средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

31) средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

32) субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа;

33) технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов

и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

34) угрозы безопасности информации – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при её обработке в информационной системе;

35) уничтожение информации – действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации;

36) уязвимость – некий недостаток, который можно использовать для нарушения системы или содержащейся в ней информации;

37) целостность информации – свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

3. В настоящей Политике используются следующие сокращения:

BIOS – базовая система ввода-вывода;

АРМ – автоматизированное рабочее место;

ИС – информационная система;

ГИС – государственная информационная система;

ГРИИБ – группа реагирования на инциденты информационной безопасности;

ИСПДн – информационная система персональных данных;

НСД – несанкционированный доступ;

КИИ – критическая информационная инфраструктура;

ПО – программное обеспечение;

СЗИ – средства защиты информации;

СКЗИ – средства криптографической защиты информации;

ТС – технические средства.

4. Уполномоченным органом ИТКС является Министерство цифрового развития Камчатского края.

5. Оператором ИТКС является краевое государственное автономное учреждение «Информационно-технологический центр Камчатского края».

6. В соответствии с указом Президента Российской Федерации от 06.03.1997 № 188 к сведениям конфиденциального характера (защищаемой информации) в ИТКС относятся:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

3) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

4) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

7. Целями настоящей Политики являются:

1) обеспечение конфиденциальности, целостности, доступности защищаемой информации;

2) обеспечение работоспособности ИТКС;

3) мониторинг событий безопасности и реагирование на инциденты безопасности;

4) нейтрализация актуальных угроз безопасности информации;

5) выполнение требований действующего законодательства по защите информации.

8. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

9. Настоящая Политика обязательна к исполнению для всех пользователей ИТКС (далее – Пользователи), в том числе с привилегированным доступом.

10. Пользователи с привилегированным доступом подразделяются на следующие категории (роли):

1) администраторы информационной безопасности (Администраторы ИБ);

2) администраторы системного и сетевого обеспечения ИТКС (Администраторы ИТКС);

3) администраторы информационных систем (Администраторы ИС);

4) администраторы сопровождения компьютерной техники (далее – Администраторы СКТ);

5) локальные системные администраторы (Администраторы сегмента ИТКС).

11. Администраторы ИБ – работники Оператора ИТКС, отвечающие за обеспечение информационной безопасности в ИТКС.

12. Администраторы ИТКС – работники Оператора ИТКС, отвечающие за системное и сетевое администрирование ИТКС.

13. Администраторы СКТ – работники Оператора ИТКС, отвечающие за сопровождение компьютерной техники.

14. Администраторы ИС – работники Абонента ИТКС, выполняющие функции администратора в информационных системах (в том числе ГИС, ИСПДн, объектов КИИ), функционирующих в ИТКС.

15. Администраторы сегмента ИТКС – работники Абонента ИТКС, должностные обязанности которых подразумевают обеспечение штатной работы парка компьютерной техники и программного обеспечения, принадлежащих им на праве собственности, аренды или ином законном основании.

16. Уполномоченный орган ИТКС наделяется следующими полномочиями:

1) проведение проверочных мероприятий по исполнению требований информационной безопасности в ИТКС;

2) разработка правовых актов и организационно-распорядительных документов по информационной безопасности в ИТКС;

3) выбор средств обеспечения информационной безопасности в ИТКС;

4) согласование внедряемых в ИТКС технических, программных и программно-технических средств защиты информации;

5) создание, развитие и администрирование системы защиты информации в ИТКС;

6) обеспечение мероприятий по обнаружению, предупреждению, ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в ИТКС.

17. Уполномоченный орган ИТКС не несет ответственности за обеспечение безопасности ИСПДн, ГИС, объектов КИИ и других информационных систем, расположенных в ИТКС, оператором которых не является.

18. Уполномоченный орган ИТКС вправе делегировать часть своих полномочий Оператору ИТКС или иным организациям с целью оптимизации использования ресурсов и наибольшего охвата мероприятиями по ИБ в части реализации собственных функций и задач. Полномочия могут быть делегированы как полностью, так и распределены по зонам ответственности между организациями, включая организации, которые осуществляют свою деятельность на правах аутсорсинга.

19. Абоненты ИТКС, в пределах своих полномочий:

1) обеспечивают выполнение требований по защите информации;

2) реализуют внедрение рекомендаций, разработанных Уполномоченным органом ИТКС;

3) осуществляют взаимодействие с Уполномоченным органом ИТКС и Оператором ИТКС в части информирования о нештатных ситуациях и инцидентах, выявленных в процессе эксплуатации информационных ресурсов ИТКС;

4) оказывают содействие работникам Уполномоченного органа ИТКС и Оператора ИТКС в части выполнения мероприятий по реагированию на инциденты информационной безопасности, корректной работе ИТКС и управлению средствами защиты информации, а также организации порядка эксплуатации средств криптографической защиты информации;

5) при необходимости осуществляют закупку дополнительных средств защиты информации.

20. Оператор ИТКС наделяется следующими полномочиями в рамках границ своих функций:

1) управление инцидентами информационной безопасности;

2) управление службами каталогов;

3) управление правами Пользователей и Администраторов;

4) управление доступом Пользователей и Администраторов к ресурсам ИТКС и сети Интернет;

5) управление средствами защиты от несанкционированного доступа;

6) управление комплексной системой антивирусной защиты;

7) управление межсетевым экранированием и системами обнаружения и предотвращения вторжений;

8) управление программным обеспечением и файлами, используемыми в ИТКС;

9) мониторинг информационных ресурсов, размещенных в ИТКС.

2. Права и обязанности администраторов

21. В зависимости от зоны ответственности Администратора в его обязанности входит:

1) знание состава, структуры, назначения и выполняемых задач информационными системами, а также состава информационных технологий и технических средств, позволяющих осуществлять обработку информации в ИТКС;

2) обеспечение передачи конфиденциальной информации и персональных данных через сети связи общего пользования в зашифрованном виде;

3) принятие мер по выполнению мероприятий по обеспечению безопасности защищаемой информации в ИТКС и непосредственное участие в проведении таких мероприятий;

4) организация первоначального доступа Пользователям к ресурсам информационных систем или ИТКС в целом. Блокировка учетных записей, изменение полномочий пользователей и добавление новых пользователей ИТКС;

5) участие в составе группы реагирования на инциденты информационной безопасности в расследованиях причин инцидентов безопасности, внесение по результатам таких расследований предложений по совершенствованию системы безопасности. По мере возможности и полномочий, Администраторы должны восстанавливать ущерб, нанесенный информационной системе во время инцидента безопасности, а также восстанавливать информацию, модифицированную или уничтоженную в результате такого инцидента;

6) контроль выполнения Пользователями ИТКС требований Инструкции пользователя ИТКС (приложение 2 к настоящей Политике), а также других установленных требований для обеспечения безопасности информации;

7) оказание необходимой помощи в подключении источников информации о событиях безопасности к центрам обеспечения безопасности (Security Operation Center (SOC);

8) изучение отчетов, полученных от SOC и своевременное реагирование на выявленные инциденты информационной безопасности;

9) обеспечение отсутствия на АРМ Пользователей ИТКС средств разработки и отладки программного обеспечения. Контроль за отключением на АРМ Пользователей и невозможностью самостоятельного включения пользователем технологий мобильного кода, кроме случаев, когда использование таких технологий необходимо для выполнения служебных (должностных) обязанностей;

10) контроль сотрудников сторонних организаций, производящих ремонт/обслуживание технических средств ИТКС или настройку/установку программного обеспечения ИТКС;

11) обеспечение непрерывности процессов в ИТКС. В случае нарушения работоспособности технических средств и программного обеспечения ИТКС, в том числе средств защиты ИТКС, принятие мер по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.

22. Администратор ИБ несет ответственность за:

1) организацию управления политиками безопасности в ИТКС (в совместной работе с Администраторами ИТКС), обновлениями антивирусных баз и сигнатур;

2) мониторинг событий безопасности в ИТКС;

3) своевременное реагирование на инциденты безопасности в ИТКС;

4) управление средствами защиты информации ИТКС, находящихся в зоне его ответственности;

5) организацию и проведение расследований информационной безопасности в ИТКС;

6) создание политик межсетевого экранирования.

23. Администратор ИБ имеет право:

1) требовать от Пользователей и Администраторов выполнения мер обеспечения безопасности информации;

2) принимать необходимые меры по нейтрализации возникающих угроз безопасности;

3) инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ИТКС;

4) требовать прекращения работы в ИТКС отдельных Пользователей и Администраторов, в случае выявления нарушений требований по обеспечению безопасности информации или в связи с нарушением функционирования ИТКС;

5) требовать от Абонентов ИТКС выполнения отдельных мер по обеспечению порядка эксплуатации средств криптографической защиты информации;

6) отказывать в запросах Администраторам если запрос противоречит политике ИБ;

7) запрашивать от Администраторов доступы, необходимые для выполнения работ в рамках ответственности.

24. Администратор ИТКС несет ответственность за:

1) обеспечение работоспособности и корректности конфигурации оборудования, на базе которого построена ИТКС;

2) обеспечение работоспособности, корректности конфигурации, доступности информационно-вычислительных ресурсов;

3) обеспечение логической связанности оборудования ИТКС;

4) обеспечение корректности настроек правил межсетевого экранирования ИТКС;

5) логические разделение ИТКС на подсети;

6) регулярность выполнения резервного копирования информационных ресурсов и целостность резервных копий;

7) сохранность информации, относящейся к рабочим процессам и расположенной на специально выделенных серверах.

25. Администратор ИТКС имеет право:

1) требовать от Администраторов и Пользователей ИТКС выполнения отдельных мер по обеспечению работоспособности ИТКС и ее взаимодействию с внешними информационными системами;

2) запрашивать от Администраторов и Пользователей ИТКС информацию, необходимую для корректной конфигурации и работоспособности оборудования;

3) запрашивать от Администраторов доступы, необходимые для выполнения работ в рамках ответственности;

4) по требованию Администраторов ИБ или при иной необходимости отключать отдельное оборудование либо информационные ресурсы от ИТКС, блокировать доступ Пользователей, Администраторов и отдельных информационных ресурсов к ИТКС и внешним информационным системам, включая сеть Интернет;

5) отказывать в запросах Администраторам, кроме Администраторам ИБ, если запрос противоречит политике ИБ и/или приведет к нарушению функционирования ИТКС.

26. Администратор ИТКС не несет ответственность за:

1) содержание проходящих по ИТКС информационных потоков;

2) работоспособность рабочих мест, подключенных к ИТКС;

3) за сохранность любой информации хранящейся на рабочих местах или оборудовании пользователя, подключенных к ИТКС.

27. Администратор СКТ несет ответственность за:

1) управление учетными записями пользователей в Домене;

2) разграничение и предоставление прав доступа к файловым ресурсам ИТКС;

3) управление рабочими местами Пользователей;

4) своевременную блокировку неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования более 45 дней;

5) установку и настройку необходимого программного обеспечения на рабочих местах Пользователей;

6) удаление устаревших записей рабочих мест Пользователей из домена;

7) техническую поддержку Пользователей ИТКС;

8) прием и обработку заявок, поступающих по адресу helpdesk.kamgov.ru, а также при необходимости их перенаправление;

9) работоспособность рабочих мест, подключенных к ИТКС;

10) исполнение всех требований Администраторов ИБ и ИТКС.

28. Администратор СКТ имеет право:

1) обращаться к Администраторам ИБ для получения информации и доступов необходимых для выполнения работ в рамках своих обязанностей;

2) требовать от пользователей доступа к оборудованию для выполнения своих обязанностей.

29. Администратор СКТ не несет ответственность за:

1) за сохранность любой информации хранящейся на рабочих местах или оборудовании, подключенных к ИТКС, а также серверах ИТКС;

2) содержание проходящих по ИТКС информационных потоков.

30. Администратор ИС несет ответственность за:

1) работоспособность информационных систем, находящихся в зоне его ответственности;

2) управление доступом пользователей к данным информационным системам;

3) обеспечение выполнения требований регуляторов в области защиты информации (ГИС, ИСПДн и т.д.);

4) отсутствие в информационных системах угроз безопасности для ИТКС (установка необходимых обновлений, закрытие уязвимостей и т.д.);

5) своевременное устранение замечаний со стороны Администраторов ИТКС и ИБ;

6) исполнение требований Администраторов ИТКС и ИБ;

31. Администратор ИС имеет право:

1) запрашивать у Администраторов ИТКС и Администраторов ИБ информацию, необходимую для корректной конфигурации и работоспособности вверенных информационных системы;

2) направлять запросы Администраторам ИТКС и Администраторам ИБ о необходимости внесения изменений в конфигурацию ИТКС или ее системы защиты для корректной работы информационной системы.

32. Администратор сегмента ИТКС несет ответственность за:

1) работоспособность оборудования и рабочих мест Пользователей исполнительного органа или подведомственного ему учреждения, работающего в ИТКС;

2) своевременное устранение замечаний со стороны Администраторов ИТКС и ИБ;

3) исполнение требований Администраторов ИТКС и ИБ;

4) обеспечение доступов необходимых для выполнения обязанностей Администраторов ИБ и ИТКС;

33. Администраторы сегмента ИТКС имеет право:

1) запрашивать у Администраторов ИТКС и Администраторов ИБ информацию, необходимую для корректной конфигурации и работоспособности оборудования и рабочих мест Пользователей;

2) направлять запросы Администраторам ИТКС и Администраторам ИБ о необходимости внесения изменений в конфигурацию ИТКС или ее системы защиты для корректной работы оборудования и рабочих мест Пользователей.

3. Правила и процедуры идентификации и аутентификации пользователей ИТКС, положение разграничения доступа к ресурсам ИТКС

34. С целью соблюдения принципа персональной ответственности за свои действия каждому Пользователю, допущенному к работе с ресурсами ИТКС, присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИТКС.

35. Под учетной записью Пользователя понимается доменная учетная запись для доступа к ИТКС.

36. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей), а также использование обезличенных учетных записей (за исключением системных) в ИТКС запрещено.

37. Процедура регистрации (создания учетной записи и выдачи, при необходимости, электронного ключа) пользователя ИТКС и предоставления ему (или изменения его) прав доступа к ресурсам ИТКС инициируется заявкой руководителя подразделения (либо лицом, его замещающим), в котором работает этот пользователь. Заявка направляется в систему учета заявок по адресу helpdesk.kamgov.ru. В заявке указывается:

1) содержание запрашиваемых изменений (регистрация нового пользователя ИТКС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИТКС ранее зарегистрированного пользователя);

2) должность (с полным наименованием подразделения), фамилия, имя и отчество работника;

3) полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИТКС);

38. в случае создания учетной записи для нового работника – скан-копию документа, подтверждающего назначение на должность, листа ознакомления работника с настоящей Политикой, а также Инструкцией Пользователя ИТКС (приложение 2 к настоящей Политике), размещенной в базе знаний корпоративного портала исполнительных органов Камчатского края.

39. Администраторы СКТ осуществляют проверку полноты предоставленной информации и корректности заявки, а также при необходимости уточняют его должностные и функциональные обязанности и

сопоставляют их с технологическими процессами обработки информации в ИТКС.

40. После этого Администраторы СКТ определяют тип учетной записи и необходимые права, формируют учетную запись и первичный пароль, сообщают пользователю идентификационные данные и допускает к работе в ИТКС. По окончании в заявке делается отметка о выполнении задания.

41. После допуска к работе в ИТКС, Пользователь самостоятельно формирует пароль доступа к своей учетной записи согласно следующим требованиям:

1) минимальная длина пароля составляет 10 символов;

2) в числе символов пароля обязательно должны присутствовать прописные буквы английского алфавита от «A» до «Z», строчные буквы английского алфавита от «a» до «z», десятичные цифры (от 0 до 10), неалфавитные символы (@, #, $, &, *, % и т.п.). Исключение составляют АРМ Роспатента, в которых использование подобных спецсимволов недопустимо;

3) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd и т.п.);

4) новый пароль должен отличаться минимум на два символа от предыдущего;

5) запрещается использование пользователями пяти последних использованных паролей при создании новых паролей.

42. Для составления сложного и хорошо запоминаемого пароля можно использовать метод парольных фраз.

Под парольной фразой понимается грамматически правильно построенное предложение, составленное из чисел и слов, помогающее сделать пароль легким для запоминания.

Например, составляем фразу «98 Сестер Одобрили Вождя», и вводим выделенные символы на английском раскладе без пробелов, соблюдая регистр, и получаем пароль «98CtcJljDj;», удовлетворяющий требованиям к паролям (п. 3.3 настоящей Инструкции).

43. Запрещено записывать и хранить пароли в местах, доступных для просмотра посторонним лицам (на отдельных листах бумаги, в не запираемой тумбе, под клавиатурой, на мониторе и т. п.).

44. Для внутренних учетных записей информационных систем (включая ГИС, ИСПДн и др.) действуют те же требования, что и для учетных записей пользователей ИТКС. Ответственность за контроль над соблюдением данных требований лежит на Администраторах данных ИС.

45. Пароли внутренних учетных записей информационных систем, установленные сотрудниками сторонних организаций, должны в оперативном порядке быть заменены после ввода данных систем в эксплуатацию либо после окончания срока действия договоров на оказываемые услуги.

46. Запрещается сохранять пароли доступа к информационным системам в браузерах и прикладном программном обеспечении.

47. Для проведения работниками сторонних организаций временных работ в ИТКС предусмотрены временные учетные записи. Все работы от имени таких учетных записей проводятся только под контролем Администраторов ИТКС, ИБ или ИС.

48. По окончании необходимых работ на удаленных рабочих столах сеансы должны быть завершены (либо самим Пользователем, либо в автоматическом режиме по окончании установленного Администраторами ИТКС промежутка времени).

49. Администратор СКТ осуществляет контроль соответствия состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа, а также контроль отсутствия незаблокированных учетных записей:

1) уволенных работников;

2) работников, отсутствующих на рабочем месте более 45 календарных дней;

3) работников внешних (подрядных) организаций, прекративших свою деятельность в организации;

4) неопределенного целевого назначения.

50. Работники кадровых служб всех Абонентов ИТКС, обязаны уведомлять Администраторов СКТ об увольняющихся работниках не позднее 3 рабочих дней до даты их фактического увольнения. Информирование производится посредством направления соответствующей заявки по адресу helpdesk.kamgov.ru.

51. В качестве модели разграничения доступа к ресурсам ИТКС выбрана ролевая модель. Пользователям назначается роль в разграничительной системе ИТКС в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от необходимости доступа к тем или иным ресурсам ИТКС. Обязанности и задачи пользователей определяются исходя из технологических процессов обработки информации в ИТКС. Описание всех возможных ролей в ИТКС приведено в приложении 1 к настоящей Политике. Помимо учетных записей Пользователей, доступ к ИТКС получают различные системные службы и процессы.

52. Идентификация и аутентификация устройств в ИТКС осуществляется по совокупности имени или ID устройства, IP-адреса и MAC-адреса. Идентификация и аутентификация устройств осуществляется с помощью механизмов межсетевого оборудования и служб управления каталогами. В случае выявления посторонних устройств, Администратор ИТКС либо ИБ оперативно блокирует доступ неустановленного устройства и созывает ГРИИБ, которая, в свою очередь, устанавливает причины и последствия такого инцидента.

53. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только Администраторам ИБ, Администраторам ИТКС и работникам сторонней организации, производящим работы в ИТКС на договорной основе под контролем вышеупомянутых администраторов. При вводе в эксплуатацию

сетевого оборудования на нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.

54. Пользователям запрещены любые действия в ИТКС до прохождения процедуры идентификации и аутентификации. Администраторам ИТКС, ИБ, ИС и Администраторам сегментов ИТКС разрешается действия до прохождения идентификации и аутентификации в ИТКС в ряде случаев:

1) загрузка операционной системы в безопасном режиме;

2) восстановление операционной системы с последней работоспособной конфигурацией;

3) изменение параметров BIOS;

4) загрузка с внешнего носителя с целью восстановления или переустановки операционной системы, восстановления работоспособности средств защиты информации, сканирования жесткого диска на вирусы, сканирования оперативной памяти или жесткого диска с целью выявления проблем и других действий восстановительного или диагностического характера.

4. Правила и процедуры управления информационными потоками

55. С целью определения разрешенных маршрутов прохождения информации между пользователями, устройствами, сегментами в рамках, а также между информационными системами и при взаимодействии с сетью Интернет устанавливаются правила и процедуры управления информационными потоками.

56. С целью управления информационными потоками в ИТКС на всех сетевых устройствах (включая сетевые адаптеры АРМ Пользователей и серверов) прописываются необходимые маршруты.

57. Администраторы ИТКС осуществляют контроль неизменности маршрутов, а также добавляет необходимые маршруты в случае необходимости.

58. Контроль и фильтрация информационных потоков между ИТКС и внешними телекоммуникационными сетями осуществляется с помощью систем межсетевого экранирования (далее – МЭ).

59. Для контроля и фильтрации трафика, входящего в ИТКС из внешних телекоммуникационных сетей, выбирается положение «Блокировать все, кроме явно разрешенного». Исходящий трафик блокируется по мере необходимости с целью исключения возможности доступа Пользователей к сайтам с вредоносным содержимым, а также к фишинговым сайтам (сайты, имитирующие другие легальные сайты с целью кражи аутентификационной и/или личной информации Пользователей).

5. Правила и процедуры антивирусной защиты информации

60. Администраторы ИБ осуществляют настройку и контроль функционирования системы антивирусной защиты в ИТКС. Управление системой осуществляется централизованно, и только Администраторы ИБ могут осуществлять такую функцию. Антивирусная защита осуществляется на АРМ, серверах, мобильных технических средствах и иных точках доступа в ИТКС.

61. Администраторы ИБ централизованно настраивают время, периодичность и другие параметры проведения полной антивирусной проверки узлов ИТКС на наличие вредоносных компьютерных программ (вирусов).

62. Администраторы ИБ самостоятельно или в составе ГРИИБ (в случае значительного инцидента безопасности) реагируют на сообщения системы антивирусной защиты или пользователей об обнаружении вредоносных компьютерных программ (вирусов), или на подозрение наличия таковых, и принимают меры по нейтрализации обнаруженных угроз.

63. Состав ГРИИБ утверждается отдельным приказом Уполномоченного органа ИТКС.

64. Администраторы ИБ настраивают периодичность обновления баз и сигнатур антивирусного средства. Администраторы ИБ также настраивают механизм распространения обновленных антивирусных баз на все узлы ИТКС. Обновление антивирусных баз и сигнатур проводится ежедневно.

65. Запрещается препятствование корректной работе системы антивирусной защиты, попытки ее деинсталляции либо ее агентов управления. Данные действия расцениваются как инциденты информационной безопасности и могут повлечь проведение служебных расследований и принятие необходимых мер на усмотрение Администраторов ИБ для нейтрализации возникающих угроз.

6. Регламентация и контроль использования технологий беспроводного доступа, защита беспроводных соединений

66. Беспроводной доступ в ИТКС применяется только по согласованию с Администраторами ИБ и ИТКС для отдельных групп устройств и пользователей, которым он необходим для выполнения своих должностных обязанностей, либо для обеспечения гостевого доступа посетителей к сети Интернет. При этом запрещено использование беспроводного доступа на местах, подключенных к государственным информационным системам.

67. Запрещается организовывать гостевой доступ посредством беспроводных соединений, подключенных к основной локальной сети ИТКС. Гостевой доступ организуется только через отдельную локальную сеть, физически отделенную от основной сети ИТКС.

68. Для обеспечения беспроводных соединений с основной сетью ИТКС должно использоваться оборудование, реализующее стандарт 802.11x и следующие функции:

1) возможность отключения функций быстрого доступа к точке беспроводного доступа (WPS, QSS и т. д.);

2) возможность отключения функции конфигурирования устройства через беспроводной канал связи;

3) возможность смены пароля администратора устройства по умолчанию.

69. Администраторы ИТКС (либо иные группы Администраторов по предварительному согласованию с Администраторами ИТКС) при первом же развертывании устройства беспроводного доступа изменяют пароль доступа к панели управления устройством, установленный по умолчанию. Новый пароль доступа к панели управления устройством должен соответствовать парольной политике и сменяться с периодичностью, установленной парольной политикой.

70. Идентификация и аутентификация Пользователей и устройств, подключающихся к информационной системе, осуществляется в соответствии с правилами, описанными в разделе 3 настоящей Политики.

71. Администратор ИТКС (либо иные группы Администраторов, получившие от Администраторов ИТКС согласие на развертывание беспроводной сети) жестко привязывают устройства пользователей к точкам беспроводного доступа и настраивает политики доступа устройства так, чтобы они запрещали пользователю изменить беспроводную точку доступа.

72. Несогласованная организация беспроводного доступа является инцидентом ИБ.

7. Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения

73. В ИТКС разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационных систем либо ИТКС в целом, а также необходимы для выполнения Пользователями своих служебных (должностных) обязанностей.

74. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только Администраторами, при этом устанавливаемое программное обеспечение не должно входить в Перечень категорий запрещенного программного обеспечения в ИТКС, разрабатываемого и утверждаемого Уполномоченным органом ИТКС. Все группы пользователей ИТКС должны быть ознакомлены с указанным перечнем под подпись. Пользователям запрещена установка любого ПО в ИТКС.

75. Пользователь либо Администратор имеют право подать заявку на включение в список исключений запрещенного в ИТКС программного обеспечения, необходимого ему для выполнения служебных (должностных) обязанностей. В такой заявке обязательно указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки составляет не более 5 рабочих дней.

76. Администраторы ИБ ежемесячно проводят проверку соответствия состава программного обеспечения в ИТКС списку запрещенного программного обеспечения. В случае выявления постороннего программного обеспечения производится его удаление либо созывается группа реагирования на инциденты информационной безопасности, которая действует в соответствии с инструкцией

по реагированию на инциденты информационной безопасности, утвержденной Уполномоченным органом ИТКС.

77. Информационная страница запрещенного в ИТКС программного обеспечения располагается в базе знаний корпоративного портала исполнительных органов Камчатского края.

8. Защита машинных носителей информации, контроль интерфейсов ввода-вывода, гарантированное уничтожение информации

78. Одной из основных целей злоумышленников являются машинные носители информации, используемые в ИТКС для хранения и обработки защищаемой информации. Исходя из этого, защита машинных носителей информации (как в стационарных АРМ и серверах, так и мобильных/съемных) является ключевым звеном политики информационной безопасности.

79. Использование съемных носителей и портативных устройств (в том числе личных), не относящихся к рабочему процессу, в ИТКС запрещено.

80. На усмотрение Администраторов ИБ либо при необходимости контроля использования съемных носителей информации в аттестованных информационных системах, функционирующих в ИТКС, могут применяться соответствующие настройки средств защиты информации. Попытки использования съемных носителей информации, неразрешенных к использованию, фиксируются средствами защиты от несанкционированного доступа либо антивирусным средством. На усмотрение Администраторов ИБ такие попытки являются инцидентами безопасности и могут расследоваться в определенном порядке.

81. USB, LPT и COM порты контролируются с помощью СЗИ от НСД либо антивирусным средством. К работе с данными интерфейсами вывода допущены пользователи в соответствии с действующей политикой учета съемных носителей информации.

82. Гарантированное уничтожение (стирание) информации на машинных носителях организовывается Администраторами в случаях:

1) передачи носителя информации в сторонние организации (в том числе и для проведения ремонта технического средства);

2) при утилизации технических средств.

83. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации. Контроль невозможности восстановления уничтоженной информации производится Администраторами с помощью специализированных утилит по восстановлению информации.

84. При передаче носителя информации в сторонние организации (не с целью передачи на нем информации), в том числе и для ремонта носителя или технического средства, информация уничтожается путем полной многократной перезаписи машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации. Затем производится очистка всего физического

пространства накопителя, включая сбойные и резервные элементы памяти, специализированными программами или утилитами производителя.

85. При утилизации технических средств, а также при возникновении необходимости уничтожения информации на неперезаписываемых машинных носителях (например, CD-R), физически уничтожается сам машинный носитель.

9. Управление взаимодействием с информационными системами сторонних организаций (внешними информационными системами)

86. Администраторы ИТКС и ИС обеспечивают управление информационными потоками при взаимодействии с внешними информационными системами.

87. Порядок обработки, хранения и передачи информации с использованием внешних информационных систем определяются технологическими процессами обработки информации в системах.

88. Взаимодействие ИТКС с информационными системами возможно только при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы.

10. Правила и процедуры применения удаленного доступа

89. В ИТКС для достижения некоторых целей и задач применяются технологии удаленного доступа к информационным системам.

90. Процедура предоставления удаленного доступа Пользователям к ресурсам ИТКС (а также внешним пользователям, которым такой доступ необходим для обновления, установки, разработки программного обеспечения и других действий в информационной системе в соответствии с договором) регламентируется отдельным порядком, утвержденным Уполномоченным органом ИТКС.

91. При работе с ресурсами ИТКС на удаленной рабочей машине запрещается подключение к сайтам, связанным с криптовалютой, tor-нодами, запуск торрент-клиентов и прочих загрузчиков.

92. В случае выявления центром мониторинга ИТКС инцидентов информационной безопасности, связанных с удаленным подключением, Пользователь обязан оказывать содействие и выполнять требования Администраторов ИБ.

93. Администраторы ИТКС и ИБ осуществляют мониторинг и контроль удаленного доступа на предмет выявления установления несанкционированного соединения технических средств (устройств) с ИТКС. В случае выявления несанкционированного доступа, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

94. С целью упрощения контроля за удаленными подключениями Администраторы ИТКС обеспечивают единую точку удаленного доступа к ИТКС.

95. Администраторы ИТКС обеспечивают защиту канала связи.

96. Администраторы ИТКС обеспечивают отсутствие возможности удаленного доступа к ИТКС по уязвимым протоколам (ftp, telnet и т. д.).

11. Правила и процедуры выявления, анализа и устранения уязвимостей

97. Полное сканирование ИТКС на выявление уязвимостей проводят Администраторы ИБ, Администраторы ИС (по согласованию с Администраторами ИБ) либо организация-лицензиат в рамках заключенных договоров.

98. Сканирование ИТКС на наличие уязвимостей проводится с периодичностью, необходимой и достаточной для должной обработки отчета по результатам сканирования и принятия мер по устранению выявленных уязвимостей, но не реже одного раза в квартал.

99. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в ИТКС необходимо организовать внеплановое полное сканирование информационной системы.

100. Администраторы ИБ и ИТКС (либо Администраторы ИС, если уязвимости обнаружены в информационных системах, находящихся в зоне их ответственности) изучают отчеты по результатам сканирования и принимают решение о немедленном устранении выявленных уязвимостей, либо о включении мероприятий по устранению выявленных уязвимостей в план мероприятий по защите информации, в случае, если выявленные уязвимости не являются критичными, или если есть возможность сделать невозможным их эксплуатацию потенциальным злоумышленником (например, путем отключения отдельных АРМ и/или сегментов сети от Интернет). При необходимости, для адекватного реагирования на вновь выявленные угрозы может созываться ГРИИБ.

101. Устранение уязвимостей в отдельных информационных системах, функционирующих в ИТКС (ГИС, ИСПДн и др.) обеспечивают Администраторы ИС.

102. Критичность уязвимостей может быть установлена как на основании рейтинга уязвимости по шкале CVSS, так и на основании оценки рисков информационной безопасности в соответствии с ГОСТ Р ИТКСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

103. При выявлении уязвимостей, Администраторы ИБ и ИТКС анализируют системные журналы и журналы средств защиты информации, на предмет выявления эксплуатации выявленной уязвимости в информационной системе и последствий такой эксплуатации.

12. Правила и процедуры контроля установки обновлений программного обеспечения

104. С целью противодействия эксплуатации известных уязвимостей, в ИТКС устанавливаются правила и процедуры контроля установки обновлений системного и прикладного программного обеспечения.

105. Автоматические обновления системного и прикладного программного обеспечения отключены.

106. Общесистемное программное обеспечение и основное прикладное программное обеспечение обновляется Администраторами ИТКС и Администраторами ИС с предварительной установкой на тестовой группе устройств, при необходимости перед обновлениями создают образы систем, точки восстановления и резервные копии баз данных.

107. Администраторы ИТКС и Администраторы ИС контролируют источники обновлений программного обеспечения. Обновления должны осуществляться из доверенных источников, в соответствии с документацией на программное обеспечение.

108. В случае необходимости для корректной установки обновлений Администраторы ИТКС и Администраторы ИБ вправе проводить перезагрузку рабочих станций пользователей в утренние часы до начала рабочего дня. Перезагрузка серверного оборудования проводится по отдельному согласованию с Администраторами ИС.

109. В случае невозможности установки критичных обновлений должны быть приняты меры, компенсирующие отсутствие данных обновлений.

110. Обновление антивирусных баз, сигнатур уязвимостей, баз решающих правил средств защиты информации осуществляется в соответствии с эксплуатационной документацией на СЗИ и разделами настоящей Политики.

111. Обновление микропрошивок и программного обеспечения BIOS/UEFI производится только при поступлении информации о критичных уязвимостях в таком программном обеспечении, применяемом в ИТКС.

13. Правила и процедуры контроля состава технических средств, программного обеспечения и средств защиты информации

112. Администраторы ИБ и ИТКС осуществляют контроль состава ТС, ПО и СЗИ, находящихся в зоне их ответственности, не реже одного раза в месяц.

113. Выявление несоответствия состава ТС, ПО и СЗИ технологическому процессу обработки информации в ИТКС является инцидентом безопасности. В случае выявления фактов несоответствия Администраторы ИБ и ИТКС устанавливают причины самостоятельно или созывают ГРИИБ.

114. В случае выявления несоответствия состава ТС, ПО и СЗИ, Администраторы ИБ и ИТКС принимают меры по оперативному исключению (восстановлению) из состава (в составе) ИТКС несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

115. Использование либо наличие установочных пакетов на рабочих местах пользователей и серверах программного обеспечения, включенного в

Перечень категорий запрещенного, может расцениваться как инцидент информационной безопасности.

14. Правила и процедуры резервирования технических средств, программного обеспечения, баз данных, средств защиты информации и их восстановления при возникновении нештатных ситуаций

116. Резервирование информационных ресурсов ИТКС (программного обеспечения, баз данных, средств защиты информации) за исключением рабочих мест пользователей осуществляется Администраторами ИТКС.

117. Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.

118. Нештатными ситуациями являются:

1) неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

а) несанкционированное изменение информации;

2) несанкционированный доступ к защищаемой информации:

а) заражение ИТКС злоумышленником программными вирусами;

б) хищение носителей информации;

в) нарушение функционирования технических средств обработки информации;

г) блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

3) дефекты, сбои, отказы, аварии технических средств и систем ИТКС;

4) дефекты, сбои, отказы программного обеспечения ИТКС;

5) сбои, отказы и аварии систем обеспечения ИТКС;

6) природные явления, стихийные бедствия:

а) термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);

б) механические факторы (повреждения зданий, землетрясения и т. д.);

в) электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

119. В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администраторами ИТКС, ИС, ИБ и ГРИИБ вырабатывается конкретный план действий с учетом текущей ситуации.

120. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

121. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

1) корректное отключение технических средств ИТКС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;

2) предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ИТКС, а также меры по замене/ремонту вышедших из строя средств и систем;

3) в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администраторы ИТКС восстанавливают их из резервных копий.

122. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями, выполняются следующие действия:

1) пользователи корректно отключают и обесточивают свои рабочие места;

2) Администраторы ИТКС и Администраторы сегмента ИТКС корректно отключают и обесточивают серверы и сетевое оборудование, а также предпринимают меры к эвакуации носителей информации и носителей резервных копий;

3) в случае нарушения корректной работы технических средств в ИТКС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;

4) в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, в результате стихийных бедствий или природных явлений, Администраторы ИТКС восстанавливают их из резервных копий;

5) в случае стихийных бедствий/природных явлений, опасных для жизни человека, в первую очередь организуется эвакуация работников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.

Приложение 1
к Политике по организации и проведению работ по обеспечению безопасности информации при ее обработке в информационно-телекоммуникационной сети исполнительных органов Камчатского края

Положение о разграничении прав доступа в ИТКС

Исходя из характера и режима обработки защищаемой информации в ИТКС определяется следующий перечень групп Пользователей, участвующих в обработке защищаемой информации. Перечень ролей и описание параметров доступа к ресурсам ИТКС приведен в таблице.

Роль	Описание параметров доступа к ресурсам ИТКС для данной роли
Администратор ИБ	Доступ на запись и чтение защищаемой информации, настройкам операционных систем, политик и средств защиты информации. Полный доступ к системным журналам, журналам средств защиты информации и другим электронным журналам сообщений. Управление пользователями и устройствами в ИТКС, их доступом к ресурсам и внешним информационным системам и сети Интернет
Администратор ИТКС	Доступ на запись и чтение защищаемой информации, настройкам операционных систем, политик и определенных средств защиты информации. Полный доступ к системным журналам, журналам определенных средств защиты информации и другим электронным журналам сообщений. Полное администрирование ИТКС, управление пользователями и устройствами в ИТКС, их доступом к ресурсам и внешним информационным системам и сети Интернет
Администратор СКТ	Доступ на запись и чтение защищаемой информации, настройкам операционных систем и специализированного программного обеспечения, на добавление пользователей и устройств в ИТКС
Администратор ИС	Доступ на запись и чтение защищаемой информации, настройкам операционных систем и серверов, обеспечивающих работу ИС, настройкам специализированного программного обеспечения и средств защиты информации, находящихся в зоне их

	ответственности, а также на управление пользователями в ИС
Администратор сегмента ИТКС	Доступ на запись и чтение защищаемой информации, настройкам операционной системы и специализированного ПО на рабочих местах пользователей. Доступ к системным журналам и другим электронным журналам сообщений, за исключением журналов средств защиты информации, находящихся в ведении Администраторов ИБ, ИТКС и ИС
Сотрудник технической поддержки	Доступ к настройкам специализированного программного обеспечения либо оборудования. Конкретные права доступа определяются отдельно согласно заключенным договорам на оказание услуг, но не в нарушение действующим правилам работы в ИТКС и под контролем Администраторов ИТКС, ИБ и ИС
Пользователь	Доступ на запись и чтение защищаемой информации при работе с прикладным программным обеспечением. Из под учетных записей с этой ролью разрешен запуск всех не системных процессов, необходимых для выполнения служебных обязанностей.
Временный пользователь	Конкретные права доступа определяются отдельно согласно выполняемым задачам, но не в нарушение действующим правилам работы в ИТКС и под контролем Администраторов ИТКС, ИБ и ИС

Приложение 2
к Политике по организации и
проведению работ по обеспечению
безопасности информации при ее
обработке в информационно-
телекоммуникационной сети
исполнительных органов
Камчатского края

Инструкция пользователя информационно-телекоммуникационной сети исполнительных органов Камчатского края

1. Общие положения

1. Несмотря на то, что многие действия по защите информации производятся прозрачно для Пользователя, он остается активным участником процесса по защите информации и является вовлеченным в процессы обеспечения информационной безопасности в ИТКС.

2. Пользователи ИТКС не являются привилегированными пользователями и получают доступ к ресурсам в соответствии с Положением о разграничении доступа в ИТКС. Каждому Пользователю предоставляется минимально необходимый для выполнения своих служебных обязанностей доступ к ресурсам ИТКС.

3. Пользователи ИТКС при работе с техническими средствами и информационными технологиями, являющимися частью ИТКС, должны соблюдать положения настоящей Инструкции.

2. Общие обязанности пользователя ИТКС

4. Пользователь в ИТКС выполняет только те действия, которые необходимы для выполнения его служебных (должностных) обязанностей. Любые посторонние действия в ИТКС запрещены.

5. Пользователь подписывает с работодателем соглашение о неразглашении конфиденциальной информации перед началом выполнения служебных обязанностей, связанных с доступом к такой информации.

6. Пользователь незамедлительно оповещает Администраторов ИБ о любой подозрительной активности в ИТКС, направляя обращение по адресу электронной почты incident@kamgov.ru.

7. Пользователю запрещено использовать личные технические средства (ноутбуки, смартфоны, планшеты, фотокамеры, флеш-носители, съемные жесткие диски и пр.) для обработки защищаемой информации.

8. Пользователь принимает участие в инструктажах по информационной безопасности, проводимыми Министерством цифрового развития Камчатского края либо уполномоченными им организациями. При получении

дополнительных материалов во время инструктажей, Пользователь самостоятельно изучает их с целью повышения своей осведомленности в вопросах информационной безопасности и защиты персональных данных.

9. В случае объективной необходимости, Пользователь участвует в составе группы реагирования на инциденты информационной безопасности в расследованиях причин инцидентов безопасности.

10. В целях блокирования возможности несанкционированного ознакомления с защищаемой информацией на экране монитора, Пользователь должен блокировать сеанс работы в ИТКС при покидании рабочего. Блокировка сеанса работы в ИТКС производится нажатием клавиш Win+L (Super + L или Ctrl + Alt + L на Linux-подобных операционных системах).

11. Пользователю запрещены любые действия в ИТКС до прохождения процедуры идентификации и аутентификации в системе (до ввода логина и пароля).

12. Пользователю запрещено изменение источника загрузки своего автоматизированного рабочего места (далее – АРМ) и загрузка АРМ с внешних носителей.

13. Антивирусная защита в ИТКС реализована прозрачно для Пользователя, установка антивирусных программ, обновление антивирусных баз, запуск антивирусных проверок, сбор информации о найденных вирусах производится Администраторами ИБ централизованно. Пользователю запрещено изменять настройки антивирусного программного обеспечения или отключать его (даже на короткое время). Пользователь должен оповещать Администраторов ИБ о любых аномалиях в работе АРМ. К таким аномалиям могут относиться:

1) загрузка другой операционной системы, сбой в загрузке операционной системы или аномально долгая загрузка операционной системы;

2) медленная работа локальной сети;

3) медленная работа глобальной сети;

4) отказ операционной системы Пользователю во входе в систему при условии правильно введенных учетных данных;

5) появление сообщений о шифровании данных на жестком диске и о требовании выкупа за расшифровку этих данных;

6) появление посторонних окон консоли командной строки (cmd.exe), открытие незапрашиваемых вкладок в браузере, самопроизвольное открытие других окон и программ в операционной системе;

7) медленная работа АРМ, быстрое исчерпание ресурсов АРМ при отсутствии ресурсоемких задач, запущенных на АРМ;

8) самопроизвольная работа курсора мыши и набора символов;

9) быстрое исчерпание свободного места на жестком диске;

10) отказ в доступе к файловой системе в целом или некоторым логическим томам в частности;

11) мерцание монитора;

12) несанкционированное появление баннеров и посторонних звуков на АРМ;

13) замена рисунка рабочего стола (за исключением централизованной замены с предварительным уведомлением Пользователей через Корпоративный портал);

14) несанкционированное открытие/закрытие CD/DVD-привода;

15) исчезновение файлов и каталогов, а также несанкционированное изменение их содержимого;

16) частое обращение к жесткому диску АРМ;

17) другие аномалии.

14. Пользователю запрещается самостоятельная установка любого программного обеспечения, даже необходимого для выполнения своих служебных (должностных) обязанностей. Установка разрешенного в ИТКС программного обеспечения осуществляется Администраторами СКТ либо Администраторами сегмента ИТКС. Также к установке и настройке программного обеспечения в ИТКС, при условии соблюдения мер по защите информации, допускаются сотрудники сторонних организаций.

15. Пользователю запрещается вести личную переписку с АРМ, а также хранить личные файлы, не относящиеся к его служебным (должностным) обязанностям и организации рабочего процесса. Вся обрабатываемая на АРМ информация может быть доступна Администраторам ИБ в рамках осуществления мониторинга и реагирования на события безопасности в ИТКС.

16. Администраторы не несут ответственность за сохранность личной и любой другой информации, не относящейся к рабочим процессам.

17. Пользователь должен пресекать попытки посторонних лиц (или лиц, не имеющих соответствующих полномочий) тем или иным образом получить доступ к его учетным данным, конфиденциальной информации в ИТКС, ключевой информации криптосредства и к любой другой защищаемой информации. Пользователь незамедлительно сообщает Администратору ИБ о подобных попытках (как удачных, так и неудачных).

18. Пользователю запрещено использовать технологии мобильного кода в обход принятых в ИТКС политик информационной безопасности.

19. Пользователь в меру своих сил и возможностей содействует проведению служебных расследований, инициированных в связи с инцидентами информационной безопасности.

20. В ИТКС действует политика управления информационными потоками и фильтрации сетевого трафика. Пользователь работает только с теми сетевыми ресурсами (сетевые папки, веб сайты и пр.), которые разрешены и работа с которыми необходима Пользователю для выполнения своих служебных (должностных) обязанностей. Пользователь имеет право сделать запрос Администраторам ИТКС на разрешение работы с заблокированными сетевыми ресурсами, обосновав необходимость внесения нового ресурса в белый список. Пользователю запрещено получать доступ к запрещенным внешним ресурсам в обход политик безопасности.

21. Пользователь принимает меры по противодействию несанкционированного просмотра защищаемой информации с экрана монитора посторонними лицами. К таким мерам относятся:

1) сворачивание окна, в котором отображена защищаемая информация или блокирование сеанса Пользователя при нахождении посторонних лиц вблизи рабочего места Пользователя с фронтальной стороны монитора;

2) ориентация монитора задней частью к дверным проемам и окнам;

3) в случае вынужденной ориентации монитора фронтальной частью к окну, Пользователь во время работы с защищаемой информацией закрывает шторы, жалюзи или рольставни.

22. Пользователь должен знать и соблюдать положения настоящей Инструкции, а также других внутренних нормативных документов в области информационной безопасности. При возникновении у Пользователя вопросов по защите информации и защите персональных данных в ИТКС, он обращается к Администраторам ИБ.

23. При работе с криптографическими средствами защиты информации Пользователь выполняет действующие требования законодательства, регламентирующие правила работы с данными средствами.

3. Правила управления идентификаторами, учетными записями и паролями

24. В ИТКС с целью обеспечения информационной безопасности внедрены политики управления идентификаторами, учетными записями и паролями.

25. Пользователь перед началом работы в ИТКС получает учетные данные (персональный идентификатор, логин, временный пароль) у Администратора СКТ. Администратор СКТ выдает учетные данные Пользователю на основании заявки, заполненной по форме, приведенной в политике информационной безопасности.

26. При первом входе в систему Пользователь изменяет первичный временный пароль, назначенный ему Администратором СКТ. Временной промежуток между выдачей временного пароля и первым входом Пользователя в информационную систему не должен составлять более одного часа. Пароли должны соответствовать требованиям Политики ИБ.

27. Максимальное время действия пароля – 90 дней. По истечении срока действия пароля, Пользователь должен придумать новый пароль, удовлетворяющий требованиям к паролям (п. 3.3 настоящей Инструкции).

28. При неудачных попытках входа, учетная запись Пользователя может быть заблокирована. Для разблокировки учетной записи Пользователю необходимо обратиться к Администраторам СКТ.

29. Пользователю запрещено записывать и хранить пароли в местах, доступных для просмотра посторонним лицам (на отдельных листах бумаги, в не запираемой тумбе, под клавиатурой, на мониторе и т. п.).

30. Пользователь должен удостовериться, что при вводе пароля никто не наблюдает за процессом ввода пароля.

31. Пользователю запрещено разглашать другим пользователям свои пароли, в том числе Администраторам.

32. Пользователю запрещено вводить свои учетные данные для предоставления возможности временной работы в ИТКС другим

Пользователями или посторонним лицам, поскольку все выполненные этими лицами действия в ИТКС будут считаться действиями, выполненными Пользователем. Ответственность за неправомерные действия таких посторонних лиц несет Пользователь.

33. Пользователю запрещено оставлять без присмотра персональный идентификатор (электронный ключ) при его наличии.

34. При подозрении на компрометацию пароля или иной идентификационной информации, Пользователь должен незамедлительно сообщить об этом Администраторам ИБ.

35. Запрещается сохранять пароли доступа к информационным системам в браузерах и прикладном программном обеспечении.

4. Противодействие методам социальной инженерии и правила работы с электронной почтой

36. Применение злоумышленником методов социальной инженерии является самым эффективным и разрушительным способом нарушения информационной безопасности на любом предприятии в обход всех технических мер по защите информации. Методы социальной инженерии направлены на использование человеческого фактора (человеческих слабостей и недостатков) с целью получения от Пользователя защищаемой информации или его учетных данных в ИТКС (логин и пароль). Злоумышленники – социальные инженеры для достижения своих целей могут эксплуатировать следующие особенности того или иного Пользователя:

1) лень;
2) спешка (паника);
3) безразличие;
4) профессиональный интерес;
5) желание;
6) жадность;
7) сострадание;
8) доверчивость;
9) страх.

37. Основным способом реализации методов социальной инженерии является обман Пользователя. Поскольку социальная инженерия нацелена на слабости человека, а не на технические недоработки или уязвимости информационной системы, наиболее эффективным методом противодействия социальной инженерии является повышение осведомленности Пользователей о методах социальной инженерии.

38. Взаимодействие социального инженера с Пользователем бывает трех типов: контактное (личное), телефонное и взаимодействие через электронные каналы связи. Наиболее распространено взаимодействие через электронные каналы связи, в особенности по электронной почте.

39. При личном и телефонном общении Пользователь должен убедиться, что разговаривает именно с тем человеком, за которого себя выдает собеседник.

При личном или телефонном взаимодействии социальный инженер обычно использует следующие тактики:

1) представившись сотрудником технической поддержки какого-либо сервиса или службы, социальный инженер сообщает Пользователю о какой-либо поломке или нарушении в функционировании того или иного необходимого в работе сервиса, вызывая тем самым панику и заставляя Пользователя сообщить свои учетные данные;

2) представившись руководителем высокого ранга, социальный инженер изображает гнев и недовольство действием или бездействием Пользователя, вынуждая сообщить учетные данные или иную конфиденциальную информацию;

3) представившись сотрудником организации, деятельность которой, так или иначе, может быть интересна Пользователю, вынуждает сообщить учетную или иную конфиденциальную информацию;

4) иные подобные тактики.

40. При взаимодействии через электронную почту, социальный инженер преследует одну из двух основных целей:

1) заражение АРМ Пользователя вредоносным программным обеспечением через запуск приложенного к письму файла или переходом по вредоносной ссылке;

2) переход Пользователя по поддельной ссылке, по которой находится точная копия формы авторизации легального сервиса, и ввод в эту форму идентификационной информации (как правило, при первом вводе логина и пароля поддельная форма сообщает о неправильном вводе пароля и перенаправляет на настоящую форму авторизации сервиса).

41. Наиболее распространенные примеры применения методов социальной инженерии с использованием каналов электронной почты:

1) письмо от налоговой инспекции с предложением установить из вложенного файла новые формы для сдачи налоговых деклараций;

2) письмо из банка о просроченном платеже по кредиту, подробности во вложенном файле;

3) письмо из суда о возбуждении административного/уголовного дела, подробности во вложении;

4) письмо от провайдера об одностороннем изменении тарифного плана, подробности во вложении;

5) письмо от банка (или любого другого учреждения) о блокировке учетной записи на сайте или личного кабинета, необходимо пройти по ссылке, ввести учетные данные и вручную разблокировать личный кабинет или учетную запись;

6) письмо от сервиса электронной почты (gmail.com, mail.ru, yandex.ru и т. п.) о грядущей блокировке почтового ящика, об исчерпании свободного места и т. д., необходимо пройти по ссылке, ввести учетные данные и выполнить некоторые действия.

42. При работе с электронной почтой в контексте противодействия методам социальной инженерии Пользователь руководствуется следующей информацией:

1) совпадение адреса отправителя электронного письма с доверенным адресом не является гарантией подлинности самого письма, поскольку поле «от кого» может быть подделано злоумышленником;

2) любые письма с вложениями являются подозрительными;

3) любые письма, в которых отсутствует альтернативная контактная информация отправителя (ФИО, должность, мобильный, рабочий телефон, почтовый адрес), являются подозрительными;

4) при получении неожидаемого электронного письма с вложением или ссылкой от якобы доверенного отправителя, необходимо по альтернативным каналам связи (лично, по телефону, через мессенджер) уточнить факт отправки такого письма;

5) государственные и иные организации (банки, операторы связи и т. д.) не уведомляют своих клиентов о каких-либо проблемах, исках, блокировках по электронной почте, это делается официальным письмом на бумажном носителе, через СМС (например, в случае подключенного онлайн банкинга) или по телефону;

6) необходимо тщательно проверять корректность ссылок, по которым просят пройти в письме, чаще всего злоумышленники используют похожие, но другие доменные имена, чтобы ввести Пользователя в заблуждение, например, заменяя букву «b» на букву «d» или цифру «1» на букву «l» и наоборот.

43. Атаки социальных инженеров могут быть веерными (нацеленными на как можно большее число жертв), так и целенаправленными (нацеленными на конкретную организацию или на конкретного человека). В случае целенаправленных атак, социальный инженер изучает информацию о потенциальной жертве и об организации из открытых источников (сайт компании, сайты партнеров и контрагентов, электронные биржи труда, социальные сети, новостные ленты и прочие ресурсы). В случае, если о Пользователе публикуется информация в открытых источниках или он сам публикует информацию о своем месте работы, роде деятельности, должностных обязанностях, Пользователь должен быть готов к применению этой информации социальным инженером против него.

44. В случае подозрения Пользователя на применение против него методов социальной инженерии, Пользователь незамедлительно сообщает о данном факте Администратору.

5. Работа со съемными носителями информации

45. Пользователю разрешается использовать только специально выделенные рабочие съемные носители информации в ИТКС (флешки, съемные жесткие диски, карты памяти и пр.).

46. При необходимости выноса съемного носителя из помещения, Пользователь обеспечивает защиту съемного носителя от утери, кражи или компрометации защищаемой информации на этом носителе.

47. В случае утери, кражи или компрометации носителя, Пользователь оперативно сообщает об этом Администратору.

48. Пользователь несет ответственность за сохранность выданных ему съемных носителей информации и за конфиденциальность защищаемой информации, записанной на него.