АДМИНИСТРАЦИЯ
УССУРИЙСКОГО ГОРОДСКОГО ОКРУГА
ПРИМОРСКОГО КРАЯ

РАСПОРЯЖЕНИЕ

11.11.2020 № 286

г. Уссурийск

Об утверждении
Политики информационной
безопасности в администрации
Уссурийского городского
округа

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказом ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и в целях совершенствования работы по защите информации в администрации Уссурийского городского округа

1. Утвердить Политику информационной безопасности в

администрации Уссурийского городского округа (прилагается).

2. Руководителям отраслевых (функциональных) органов администрации Уссурийского городского округа организовать работу в соответствии с настоящим распоряжением.

3. Управлению информатизации и организации предоставления муниципальных услуг администрации Уссурийского городского округа (Панченко) разместить настоящее распоряжение на официальном сайте администрации Уссурийского городского округа.

Глава Уссурийского городского округа Е.Е. Корж

УТВЕРЖДЕНА

распоряжением администрации
Уссурийского городского округа
от 11.11.2020 № 286

Политика информационной безопасности в администрации Уссурийского городского округа

I. Общие положения

1. Политика информационной безопасности в администрации Уссурийского городского округа (далее - Политика) разработана в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информатизации и защите информации», Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», приказом ФСТЭК России от 11 февраля 2013 года № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК России от 18 февраля 2013 года № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и определяет мероприятия, процедуры и правила по защите информации в информационных системах администрации Уссурийского городского округа.

2. Положения настоящей Политики распространяются на все государственные и муниципальные информационные системы администрации Уссурийского городского округа, в том числе сегменты государственных (региональных) информационных систем, подключаемых в администрации Уссурийского городского округа (далее – ИС).

При обработке в ИС персональных данных в дополнение к настоящей Политики необходимо руководствоваться Положением по обеспечению безопасности персональных данных в администрации Уссурийского городского округа, утвержденном постановлением администрации Уссурийского городского округа от 17 декабря 2013 года № 4261.

3. Целями настоящей Политики являются:

а) обеспечение конфиденциальности, целостности, доступности защищаемой информации;

б) предотвращение утечек защищаемой информации;

в) мониторинг событий безопасности и реагирование на инциденты безопасности;

г) нейтрализация актуальных угроз безопасности информации;

д) выполнение требований действующего законодательства по защите информации.

4. 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.

Пользователями ИС являются сотрудники администрации, допущенные к работе в ИС.

Администраторы ИС – это сотрудники администрации, осуществляющие подключение и настройку доступа сотрудникам администрации к ресурсам ИС.

Администраторы безопасности ИС – это сотрудники администрации,

уполномоченные на проведение работ по защите информации и поддержанию достигнутого уровня защищенности (класса) ИС администрации и ее информационных ресурсов.

5. Положения настоящей Политики обязательны к исполнению для всех пользователей ИС (далее – Пользователи), а также для администраторов безопасности и администраторов информационных систем (далее – Администраторы).

II. Технологические процессы обработки защищаемой информации в информационных системах

6. Администраторы и Пользователи, допущенные к обработке той или иной защищаемой информации, обязаны производить обработку этой информации в соответствии с описаниями технологических процессов обработки информации, приведенных в данном разделе.

7. Субъектами доступа ИС являются Пользователи, Администраторы.

Объектами доступа ИС являются текстовые, табличные и графические файлы пользователей, размещаемые на жестком магнитном диске рабочей станции и съемных носителях.

8. Средствами обработки и перемещения информации в ИС являются:

а) штатные программные средства, предоставляющие субъектам документированные возможности доступа к объектам доступа;

б) штатные технические средства, предоставляющие субъектам документированные возможности доступа к объектам доступа.

Перечень технических средств, программных средств и средств защиты информации, используемых в ИС, указывается в Техническом паспорте на ИС.

9. Технологический процесс обработки информации в ИС может включать следующие операции:

а) вход в систему при предъявлении персонального идентификатора

и/или после ввода пользователем персонального пароля;

б) ввод информации с накопителей на жестких магнитных дисках (далее – НЖМД) или съемного машинного носителя (DVD/CD-диска и USB-накопителя) или клавиатуры;

в) непосредственную обработку информации с использованием прикладного программного обеспечения и создание документов;

г) сохранение разработанных документов в отведенных каталогах на НЖМД или на съемных машинных носителях (DVD/CD-диск, USB-накопитель), либо печать документа на бумажный носитель;

д) передача защищаемой информации во внешние информационные системы.

III. Правила и процедуры идентификации и аутентификации пользователей ИС, политика разграничения доступа к ресурсам ИС

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

В качестве учетной записи Пользователя понимается учетная запись для доступа к ИС в домене Active Directory.

11. Порядок предоставления доступа к ИС администрации (далее – Порядок) утвержден распоряжением администрации Уссурийского городского округа от 21 мая 2020 года № 180 «Об утверждении Положения о разграничении прав доступа к информационным системам администрации Уссурийского городского округа и признании утратившим силу некоторых правовых актов».

12. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ИС запрещено.

13. При регистрации Пользователя Администратор:

а) определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная, учетная запись приложения, временная, гостевая) и производит необходимые настройки средств защиты от несанкционированного доступа (далее – СЗИ от НСД) и формирует учетную запись;

б) направляет Пользователю инструкцию Пользователя ИС, идентификационные данные для допуска к работе в ИС.

14. Для проведения временных работ в ИС сотрудниками сторонних организаций предусмотрена временная учетная запись с правами, необходимыми для выполнения работ. Данная учетная запись отключена и активируется только при необходимости. Все работы от имени такой учетной записи проводятся только под контролем Администратора.

15. Пользователям назначается роль в разграничительной системе ИС в зависимости от выполняемых должностных обязанностей, задач и в зависимости от необходимости по доступу к тем или иным ресурсам ИС. Обязанности и задачи пользователей определяются исходя из технологических процессов обработки информации в ИС.

Описание всех возможных ролей в ИС приведено в Приложении № 1 к настоящей Политике. Помимо учетных записей Пользователей доступ к системе получают различные системные службы и процессы.

16. Администратор обеспечивает оперативное обновление и актуальность следующих перечней в соответствии с Порядком:

а) перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ИС администрации;

б) перечень помещений, в которых разрешена работа с ресурсами ИС, в которых размещены технические средства ИС, а также перечень лиц, допущенных в эти помещения.

17. Идентификация и аутентификация на сетевом оборудовании разрешена только администраторам безопасности, администраторам системы

и сотрудникам сторонней организации, производящим работы в сети администрации Уссурийского городского округа на договорной основе под контролем Администратора. 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.

18. Пользователям запрещены любые действия в ИС до прохождения процедуры идентификации и аутентификации в системе.

IV. Правила и процедуры управления информационными потоками ИС

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

20. Контроль и фильтрация информационных потоков между ИС и внешними телекоммуникационными сетями осуществляется с помощью сертифицированного межсетевого экрана.

Для контроля и фильтрации информационных потоков между ИС и внешними телекоммуникационными сетями выбирается политика «Блокировать все, кроме явно разрешенного».

21. Для каждой ИС Администратором составляется список разрешающих правил взаимодействия с внешними телекоммуникационными сетями по форме, приведенной в Приложении № 2 к настоящей Политике.

Данный список может быть дополнен на основании служебной записки Пользователя Администратору с указанием обоснования добавления того или иного ресурса/сайта/протокола/порта в список разрешенных.

22. Администратор обеспечивает соответствие настроек межсетевого экрана списку разрешительных правил.

V. Правила и процедуры управления установкой (инсталяцией) компонентов программного обеспечения

23. В ИС разрешено использование только программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования ИС, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.

24. Для каждой ИС Администратором составляется Перечень разрешенного программного обеспечения в ИС по форме, приведенной в Приложении № 3 к настоящей Политике.

25. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется Администратором. Пользователям запрещена установка любого программного обеспечения (далее - ПО) в ИС.

26. Пользователь имеет право подать Администратору заявку на включение в список разрешенного в ИС ПО, необходимых ему для выполнения должностных обязанностей программ, утилит, драйверов с обязательным обоснованием необходимости включения в этот список нового ПО. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.

27. Администратор не реже одного раза в квартал с помощью инструмента сканер уязвимостей (Сканер-ВС или эквивалент) проводит проверку соответствия состава ПО в ИС списку разрешенного ПО. В случае выявления постороннего ПО, созывается группа реагирования на инциденты информационной безопасности (далее – ГРИИБ), которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности, утвержденной распоряжением администрации Уссурийского городского округа от 08 октября 2015 года № 270 «Об утверждении инструкций по обеспечению информационной безопасности в администрации Уссурийского городского округа».

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

28. Учет, использование, передача и уничтожение машинных носителей информации в ИС администрации должно осуществляться в соответствии с инструкцией о порядке эксплуатации электронных носителей информации, утвержденной распоряжением администрации Уссурийского городского округа от 08 октября 2015 года № 270 «Об утверждении инструкций по обеспечению информационной безопасности в администрации Уссурийского городского округа».

29. Учет машинных носителей осуществляется Администратором в соответствующих журналах. Администратор несет ответственность за достоверность и своевременность сведений, отраженных в журнале учета машинных носителей информации.

В ИС администрации учету подлежат:

а) съемные машинные носители информации (флэш-накопители, внешние НЖМД и иные подобные устройства);

б) портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

в) машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

30. При использовании в составе одного технического средства ИС нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

31. Использование неучтенных съемных носителей и/или портативных устройств (в том числе личных) в ИС запрещено.

32. Невозможность использования неучтенных съемных носителей

информации обеспечивается путем программных настроек СЗИ от НСД. Настройками СЗИ от НСД неучтенные носители информации блокируются на всех стационарных устройствах ИС. Попытки использования неучтенных съемных носителей информации фиксируются СЗИ от НСД и являются инцидентами безопасности и расследуются в соответствии с инструкцией по реагированию на инциденты информационной безопасности в администрации Уссурийского городского округа, утвержденной распоряжением администрации Уссурийского городского округа от 08 октября 2015 года № 270 «Об утверждении инструкций по обеспечению информационной безопасности в администрации Уссурийского городского округа».

33. Невозможность использования неучтенных портативных вычислительных устройств обеспечивается путем организации аутентификации в системе не только пользователя, но и самого устройства по нескольким параметрам (имя устройства, IP-адрес, MAC-адрес и другие).

34. Невозможность использования неучтенных машинных носителей в стационарных устройствах обеспечивается путем физического контроля доступа в соответствии с инструкциями Пользователя и Администратора, а также путем проведения периодических мероприятий по инвентаризации ресурсов ИС и комплектности технических средств.

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

35. ИС администрации могут осуществлять взаимодействие с внешними информационными системами.

36. Администратор обеспечивает доступ пользователей внешних информационных систем к ресурсам ИС администрации в соответствии с правилами и процедурами, описанными в разделе 3 настоящей Политики.

37. Администратор обеспечивает управление информационными

потоками при взаимодействии с внешними информационными системами в соответствии с правилами и процедурами, описанными в разделе 4 настоящей Политики.

38. Администратор составляет список прикладного программного обеспечения, доступного для конкретного перечня пользователей внешних информационных систем, в соответствии с формой, приведенной в Приложении № 4 к настоящей Политике, с указанием целей предоставления такого доступа.

39. Порядок обработки, хранения и передачи информации с использованием внешних информационных систем определяются технологическими процессами обработки информации, описанными в разделе 2 настоящей Политики.

40. Доступ к ИС пользователями внешних информационных систем и разрешение обработки, хранения и передачи информации с использованием внешних информационных систем в администрации возможно только при выполнении следующих условий:

при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

VIII. Правила и процедуры выявления, анализа и устранения уязвимостей

41. В администрации в качестве средства выявления уязвимостей используется сертифицированный сканер уязвимостей Сканер-ВС (или эквивалент).

42. Администратор не реже одного раза в квартал проводит полное сканирование ИС на выявление уязвимостей. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в ИС производится внеплановое обновление базы данных сканера уязвимостей и полное сканирование информационной системы.

43. Администратор изучает отчеты по результатам сканирования и принимает 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 Интернет). При необходимости на вновь выявленные угрозы может созываться ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности, утвержденной распоряжением администрации Уссурийского городского округа от 08 октября 2015 года № 270 «Об утверждении инструкций по обеспечению информационной безопасности в администрации Уссурийского городского округа».

44. При выявлении уязвимостей Администратор анализирует системные журналы и журналы средств защиты информации на предмет выявления эксплуатации выявленной уязвимости в ИС и последствий такой эксплуатации.

45. В случае невозможности оперативного устранения критичной уязвимости Администратор уведомляет об этом непосредственного руководителя.

IX. Правила и процедуры контроля установки обновлений программного обеспечения

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

47. В программном обеспечении, поддерживающем автоматические обновления, таких как Java, Acrobat Reader и т. д. автоматические обновления не отключаются.

48. Общесистемное программное обеспечение и основное прикладное программное обеспечение обновляется во внерабочее время.

Обновления общесистемного и основного прикладного программного обеспечения осуществляются не реже одного раза в неделю. Экстренные обновления осуществляются в случае поступления информации о критичных уязвимостях, для которых существует обновление безопасности.

49. Администратор контролирует источники обновлений программного обеспечения. Обновления должны осуществляться из доверенных источников, в соответствии с документацией на программное обеспечение.

50. Администратор в соответствии с эксплуатационной документацией на программное обеспечение осуществляет проверку установки обновлений, а также корректность установки обновлений. В администрации должно применяться только такое программное обеспечение, которое поддерживает проверку целостности файлов обновлений.

51. Обновление антивирусных баз, сигнатур уязвимостей, баз решающих правил средств защиты информации осуществляется в соответствии с эксплуатационной документацией на средства защиты информации (далее – СрЗИ).

52. Обновление микропрошивок (микрокодов/прошивок) и программного обеспечения BIOS/UEFI производится только при поступлении информации о критичных уязвимостях в таком программном обеспечении, применяемом в администрации.

X. Правила и процедуры контроля состава технических средств,

программного обеспечения и средств защиты информации

53. Состав технических средств (далее – ТС), ПО и СрЗИ ИС фиксируется в техническом паспорте на ИС. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

В случае добавления новых ТС, ПО и СрЗИ в состав ИС или удаления существующих компонентов на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) вносятся изменения в Технический паспорт.

54. Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в квартал.

55. Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ИС является инцидентом безопасности и расследуется в соответствии с инструкцией по реагированию на инциденты информационной безопасности в администрации, утвержденной распоряжением администрации Уссурийского городского округа от 08 октября 2015 года № 270 «Об утверждении инструкций по обеспечению информационной безопасности в администрации Уссурийского городского округа».

56. В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе) ИС несанкционированно установленных (удаленных) ТС, ПО и СрЗИ.

57. Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия СрЗИ и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом начальнику

отдела информационной безопасности администрации Уссурийского городского округа, который принимает решение об организации самостоятельной сертификации использующегося СрЗИ либо об обновлении использующегося СрЗИ до актуальной версии, либо о замене использующегося СрЗИ на другое аналогичное сертифицированное СрЗИ.

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

58. Инструкция по резервированию и восстановлению работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации администрации утверждена распоряжением администрации Уссурийского городского округа от 08 октября 2015 года № 270 «Об утверждении инструкций по обеспечению информационной безопасности в администрации Уссурийского городского округа».

59. Восстановление из резервных копий является основным методом восстановления работоспособности ИС после ликвидации нештатных ситуаций.

60. Нештатными ситуациями являются:

а) разглашение информации ограниченного доступа сотрудниками администрации, имеющими к ней право доступа, в том числе:

- разглашение информации лицам, не имеющим права доступа к защищаемой информации;
- передача информации по незащищенным каналам связи;
- обработка информации на незащищенных технических средствах обработки информации;
- опубликование информации в открытой печати и других средствах массовой информации;

– передача носителя информации лицу, не имеющему права доступа к ней;

– утрата носителя с информацией.

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

– несанкционированное изменение информации;

– несанкционированное копирование информации;

в) несанкционированный доступ к защищаемой информации:

– несанкционированное подключение технических средств к средствам и системам ИС;

– использование закладочных устройств;

– использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ИС;

– использование злоумышленником уязвимостей программного обеспечения ИС;

– использование злоумышленником программных закладок;

– заражение ИС злоумышленником программными вирусами;

– хищение носителей информации;

– нарушение функционирования технических средств обработки информации;

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

г) дефекты, сбои, отказы, аварии технических средств и систем ИС;

д) дефекты, сбои, отказы программного обеспечения ИС;

е) сбои, отказы и аварии систем обеспечения ИС;

ж) природные явления, стихийные бедствия:

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

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

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

61. 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.

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

– корректное отключение технических средств ИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;

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

– в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

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

– Пользователи корректно отключают и обесточивают свои рабочие места;

– системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;

– Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;

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

– в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;

– в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.

64. Перечень мероприятий по обеспечению непрерывности функционирования информационной системы, а также сроки проведения их при обнаружении нештатной ситуации отражены в Приложении № 5 к настоящей Политике.

65. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации Администраторами могут проводиться регулярные тренировки по различным видам нештатных ситуаций.

XII. Правила и процедуры применения удаленного доступа

66. В ИС администрации могут применяться технологии удаленного доступа к ИС.

67. Удаленный доступ к ИС предоставляется только тем Пользователям, которым это необходимо для выполнения своих должностных обязанностей, либо внешним пользователям, не являющимся работниками администрации, которым такой доступ необходим для обновления, установки, разработки ПО (и других действий в ИС) в соответствии с заключенным договором (контрактом).

68. Удаленный доступ к ИС запрещен от имени привилегированных учетных записей (учетных записей Администраторов).

69. Удаленный доступ к ИС предоставляется на основании списка, составленного Администратором по форме согласно Приложению № 6 к настоящей Политике.

70. С целью упрощения контроля за удаленными подключениями Администратор обеспечивает единую точку удаленного доступа к ИС.

71. Администратор обеспечивает защиту канала связи при удаленном доступе с помощью сертифицированных средств криптографической защиты.

Администратор обеспечивает невозможность получения удаленного доступа к ИС, если на удаленном рабочем месте Пользователя не установлено (или отключено) сертифицированное средство криптографической защиты.

72. Администратор обеспечивает отсутствие возможности удаленного доступа к ИС по уязвимым протоколам (ftp, telnet и т. д.).

73. Перед предоставлением удаленного доступа к ИС Администратор проводит инструктаж Пользователей по вопросам информационной безопасности.

Приложение № 1

к Политике информационной безопасности в администрации Уссурийского городского округа

Перечень ролей и описание параметров
доступа к ресурсам информационной системы

_____

(наименование информационной системы)

Исходя из характера и режима обработки защищаемой информации в информационной системе определяется следующий перечень групп Пользователей, служб и процессов, участвующих в обработке защищаемой информации:

Роль	Описание параметров доступа к ресурсам ИС для данной роли
Администратор безопасности	Полный доступ к ресурсам ИС, настройкам ОС и СЗИ. Полный доступ к системным журналам, журналам средств защиты информации и другим электронным журналам сообщений.
Администратор информационной системы	Полный доступ к ресурсам ИС за исключением доступа к настройкам СЗИ и к журналам средств защиты информации.
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.
Сканер-ВС	Доступ на чтение к системному реестру Windows. Доступ на чтение файловой структуры и папок на жестких дисках. Доступ на запись во временную директорию %SystemRoot%\Temp.

_____

Приложение № 2

к Политике информационной безопасности в администрации Уссурийского городского округа

Список разрешающих правил взаимодействия с внешними телекоммуникационными сетями в информационной системе

_____

(наименование информационной системы)

№ п/п	IP/URL ресурса, подсеть или протокол	Обоснование разрешения	Правило	Время действия правила	Учетные записи, устройства, процессы, для которых действует правило
1.					
2.					
3.					
4.					
5.					
6.					

_____

Приложение № 3

к Политике информационной безопасности в администрации Уссурийского городского округа

Список разрешенного программного обеспечения,
используемого в информационной системе

_____

(наименование информационной системы)

№ п/п	Наименование ПО	Тип ПО	Цель применения ПО в МИС	Место установки компонентов ПО
1.				
2.				
3.				
4.				
5.				

Приложение № 4

к Политике информационной безопасности в администрации Уссурийского городского округа

Список прикладного программного обеспечения,
доступного внешним пользователям информационной системы

_____

(наименование информационной системы)

№ п/п	Наименование программного обеспечения	Тип программного обеспечения	Цель допуска к программному обеспечению внешних пользователей
1.			
2.			
3.			
4.			
5.			
6.			

_____

Приложение № 5

к Политике информационной безопасности в администрации Уссурийского городского округа

План обеспечения непрерывности функционирования информационной системы

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
1.	Разглашение защищаемой информации сотрудниками, имеющими легальны права доступа к ней		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
2.	Обнаружение несанкционированно скопированной или измененной конфиденциальной информации		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
3.	Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц, имеющих право доступа к ней		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	Сразу после получения информации об инциденте	1 день
4.	Обнаружение подключения технических средств к средствам и системам объекта информатизации		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	3 часа
5.	Подключение технических средств к средствам и системам ГИС в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	Сразу после получения информации об инциденте	3 часа

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
6.	Обнаружение закладочных устройств		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	Сразу после получения информации об инциденте	1 день
7.	Установка закладочных устройств злоумышленником в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
8.	Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
9.	Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
10.	Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
11.	Использование программных закладок внешним нарушителем в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
12.	Использование программных закладок внутренним злоумышленником или обнаружение факта использования		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
13.	Обнаружение программных вирусов		Администратору сразу после	Администратору не позднее 8	10 минут в рабочее время	12 часов

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
			обнаружения инцидента	часов после инцидента	(1 час в нерабочее)	
14.	Хищение носителя защищаемой информации		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 сутки	3 дня
15.	Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
16.	Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
17.	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	7 дней
18.	Блокирование доступа к защищаемой		Администратору	Администратору	20 минут в	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
	информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени		сразу после обнаружения инцидента	не позднее 8 часов после инцидента	рабочее время (1 час в нерабочее)	
19.	Обнаружение произошедшего факта блокировки доступа к защищаемой информации		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
20.	Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	2 часа в рабочее время (12 часов в нерабочее)	1 день
21.	Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	20 минут	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	20 минут	1 день
22.	Дефекты, сбои, отказы, аварии ТС, программных средств и систем ГИС	Сбой ТС и систем ГИС	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	1 час	2 дня
		Отказ ТС и систем ГИС,	Администратору сразу после	Администратору не позднее 8	1 час в рабочее время (8 часов	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
		затронувший работу группы пользователей	обнаружения инцидента	часов после инцидента	в нерабочее)	
		Отказ ТС и систем ГИС, затронувший работу одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	1 час	2 дня
		Авария ТС и систем ГИС	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
23.	Сбои, отказы и аварии систем обеспечения ГИС	Сбой систем обеспечения ГИС	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента	1 час	1 день
		Отказ систем обеспечения ГИС, затронувший работу группы пользователей	Ответственному за материально-техническое обеспечение и Администратору сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение и Администратору сразу после обнаружения инцидента	1 час	1 день
		Отказ систем обеспечения	Ответственному за материально-	Ответственному за материально-	1 час	2 дня

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
		ГИС, затронувший работу одного пользователя	техническое обеспечение сразу после инцидента	техническое обеспечение в первый рабочий день после инцидента		
		Авария систем обеспечения ГИС	Ответственному за материально-техническое обеспечение, Администратору сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение, Администратору не позднее 8 часов после инцидента	1 час	1 день
24.	Природные явления, стихийные бедствия, несущие угрозу жизни человека		Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	10 минут	30 минут
25.	Природные явления, стихийные бедствия, не несущие угрозу жизни человека		Руководителю, заместителям Руководителя, Администратору	Руководителю, заместителям Руководителя, Администратору	10 минут	1 час

Приложение № 6

к Политике информационной безопасности в администрации Уссурийского городского округа

Список пользователей и внешних пользователей, которым в соответствии с должностными обязанностями предоставлен удаленный доступ к информационной системе

_____

(наименование информационной системы)

№ п/п	ФИО	Наименование организации	Ресурсы, к которым предоставляется удаленный доступ	Обязанности, в связи с которыми предоставляется удаленный доступ или основание для предоставления удаленного доступа	Учетная запись, от имени которой предоставляется удаленный доступ	Время, на которое предоставляется удаленный доступ
1.						