ПРАВИТЕЛЬСТВО
АМУРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

13.06.2023 № 528

г. Благовещенск

О централизованной системе
антивирусной защиты
информации

В целях совершенствования системы защиты информации в органах государственной власти Амурской области Правительство Амурской области
п о с т а н о в л я е т:

1. Утвердить Положение о централизованной системе антивирусной защиты информации согласно приложению к настоящему постановлению.

2. Контроль за исполнением настоящего постановления возложить на заместителя председателя Правительства Амурской области Пузанова П.И.

3. Настоящее постановление подлежит официальному опубликованию на «Официальном интернет-портале правовой информации» (www.pravo.gov.ru) и размещению на Портале Правительства Амурской области в информационно-телекоммуникационной сети Интернет (www.amurobl.ru).

Губернатор Амурской области Орлов

ПРАВИТЕЛЬСТВО АМУРСКОЙ ОБЛАСТИ
АППАРАТ ГУБЕРНАТОРА ОБЛАСТИ И ПРАВИТЕЛЬСТВА ОБЛАСТИ
Отдел регистрации и сопровождения правовых актов

Приложение
УТВЕРЖДЕНО
постановлением Правительства
Амурской области
от 13.06.2013 № 528

ПОЛОЖЕНИЕ
о централизованной системе антивирусной защиты информации

1. Общие положения

1.1. Настоящее Положение определяет назначение, структуру централизованной системы антивирусной защиты информации (далее – централизованная система) и функциональные обязанности ее участников.

1.2. Централизованная система представляет собой комплекс программных и технических средств, направленный на обеспечение защищенности информационных ресурсов участников централизованной системы от воздействия вредоносных компьютерных программ (вирусов), обнаружение вредоносных компьютерных программ (вирусов), а также предотвращение модификации информационных ресурсов участников централизованной системы вредоносным кодом.

1.3. В настоящем Положении используются следующие основные понятия:

1) автоматизированное рабочее место – персональный компьютер пользователя централизованной системы с периферийным оборудованием и установленным программным обеспечением;

2) сервер – специализированный компьютер (виртуальная машина) участника централизованной системы для выполнения на нем сервисного программного обеспечения, используемый одновременно множеством пользователей, совместимый с программным обеспечением централизованной системы, а также имеющий техническую возможность для подключения к централизованной системе;

3) сервер администрирования централизованной системы – средство централизованного управления системой антивирусной защиты информации, позволяющее настраивать все компоненты системы антивирусной защиты информации;

4) сервер администрирования субъекта централизованной системы – средство управления системой антивирусной защиты информации субъекта централизованной системы, позволяющее настраивать все компоненты системы антивирусной защиты информации субъекта централизованной системы;

5) вредоносная компьютерная программа (вирус) – программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам или к информации с целью несанкционированного использования ресурсов или причинения вреда (нанесения ущерба) владельцу

информации и (или) владельцу вычислительных ресурсов путём копирования, искажения, удаления или подмены информации;

6) субъект централизованной системы – орган исполнительной власти Амурской области, не являющийся централизованным органом исполнительной власти Амурской области, Законодательное Собрание Амурской области, учреждения, подведомственные министерству здравоохранения Амурской области;

7) централизованный орган исполнительной власти Амурской области – орган исполнительной власти Амурской области, находящийся на централизованном информационном обеспечении в соответствии с постановлением Губернатора Амурской области от 28.09.2018 № 230 «Об оптимизации деятельности аппарата Губернатора области и Правительства области, исполнительных органов государственной власти области»;

8) объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

1.4. Координатором централизованной системы является министерство цифрового развития и связи Амурской области.

1.5. Оператором централизованной системы является государственное бюджетное учреждение Амурской области «Центр информационных технологий Амурской области».

1.6. Участниками централизованной системы являются централизованный орган исполнительной власти Амурской области и субъект централизованной системы, подключенные к централизованной системе.

1.7. В централизованной системе определены следующие роли:

1) администратор централизованной системы – работник оператора централизованной системы, определенный ответственным за эксплуатацию централизованной системы;

2) администратор антивирусной защиты – работник участника централизованной системы, определенный ответственным за проведение мероприятий по антивирусной защите информации;

3) пользователи централизованной системы – работники участника централизованной системы, использующие в работе автоматизированные рабочие места.

1.8. Централизованная система не предназначена для обеспечения защиты информации ограниченного доступа. Для объектов информатизации, принадлежащих участникам централизованной системы и обрабатывающих информацию ограниченного доступа, настоящее Положение применяется только в части приобретения оператором централизованной системы прав использования (лицензий) средств антивирусной защиты.

2. Назначение централизованной системы

2.1. Централизованная система предназначена для организации защиты от внедрения на объекты информатизации участников централизованной системы вредоносной компьютерной программы (вирусов) и реализации единой политики антивирусной защиты информации.

2.2. Централизованная система обеспечивает мониторинг работы и управление антивирусным программным обеспечением, оптимизирует процесс распространения обновлений и мониторинга состояния антивирусной защиты информации.

3. Структура централизованной системы

3.1. Структура централизованной системы состоит из следующих элементов:

1) главный сервер администрирования централизованной системы, развернутый в структуре оператора централизованной системы, в функции которого входит:

а) распространение лицензионного ключа средства антивирусной защиты на все подчиненные сервера администрирования централизованной системы, автоматизированные рабочие места и сервера объектов информатизации;

б) получение и распространение обновлений сигнатур антивирусных баз на подчиненные серверы;

в) мониторинг событий информационной безопасности, возникающих на подчиненных серверах администрирования централизованной системы;

г) формирование отчетов о состоянии централизованной системы;

д) формирование базовых направлений функционирования средств антивирусной защиты;

е) централизованное управление средствами антивирусной защиты объектов информатизации;

ж) хранение информации о конфигурации клиентских устройств;

з) организация хранилищ дистрибутивов средств антивирусной защиты;

и) удаленная установка и удаление средств антивирусной защиты на клиентские устройства;

к) обновление баз и модулей средств антивирусной защиты;

л) управление задачами на автоматизированном рабочем месте и серверах объектов информатизации;

м) хранение информации о событиях, произошедших на автоматизированном рабочем месте и серверах объектов информатизации;

н) формирование отчетов о работе средств антивирусной защиты;

о) отправка уведомлений о событиях, произошедших на автоматизированном рабочем месте и серверах объектов информатизации в систему сбора и корреляции событий информационной безопасности;

2) общий сервер администрирования централизованной системы, на котором разворачиваются виртуальные серверы администрирования субъектов централизованной системы, которые выполняют следующие функции:

а) централизованное управление средствами антивирусной защиты объекта информатизации субъекта централизованной системы;

б) хранение информации о конфигурации клиентских устройств;

в) организация хранилищ дистрибутивов средств антивирусной защиты;

г) удаленная установка и удаление средств антивирусной защиты на клиентские устройства;

д) обновление баз и модулей средств антивирусной защиты;

е) управление задачами на автоматизированном рабочем месте и серверах объекта информатизации;

ж) хранение информации о событиях, произошедших на автоматизированном рабочем месте и серверах объектов информатизации;

з) формирование отчетов о работе средств антивирусной защиты;

и) распространение лицензионных ключей средств антивирусной защиты на автоматизированные рабочие места и сервера объекта информатизации;

к) отправка уведомлений о событиях, произошедших на автоматизированном рабочем месте и серверах объекта информатизации на общий сервер администрирования централизованной системы;

3) средства антивирусной защиты, устанавливаемые на компоненты объектов информатизации (серверах, автоматизированных рабочих местах), в функции которых входит:

а) защита от вредоносных компьютерных программ (вирусов);

б) обновление сигнатур антивирусных баз.

3.2. Для построения централизованной системы антивирусной защиты используются сертифицированные Федеральной службой по техническому и экспортному контролю средства антивирусной защиты и программное обеспечение по их централизованному администрированию.

4. Функциональные обязанности координатора централизованной системы, оператора централизованной системы, участников централизованной системы

4.1. Координатор централизованной системы обеспечивает:

1) утверждение Регламента работы централизованной системы, которым определяется порядок взаимодействия оператора централизованной системы и участников централизованной системы (с учетом разделения ролей), а также порядок взаимодействия компонентов централизованной системы (далее – Регламент);

2) методическое и организационное сопровождение централизованной системы;

3) анализ статистических показателей мониторинга функционирования централизованной системы, подготовку предложений по устранению выявленных нарушений и модернизации централизованной системы;

4) принятие правовых актов, регламентирующих вопросы создания, организации работы и эксплуатации централизованной системы;

5) осуществление контроля исполнения участниками централизованной системы мероприятий по антивирусной защите.

4.2. Оператор централизованной системы обеспечивает:

1) приобретение прав использования (лицензий) средств антивирусной защиты для всех участников централизованной системы в рамках субсидии на выполнение государственного задания на соответствующий финансовый год, доведенной до оператора централизованной системы;

2) функционирование централизованной системы в соответствии с требованиями законодательства Российской Федерации в области информации, информационных технологий и защиты информации;

3) назначение администратора (ов) централизованной системы;

4) выполнение работ по установке, настройке, обновлению, сопровождению, контролю эксплуатации, устранению сбоев в работе на главном и общем серверах администрирования централизованной системы;

5) контроль состояния антивирусной защиты информации на главном и общем серверах администрирования централизованной системы;

6) мониторинг применения установленных правил антивирусной защиты информации;

7) анализ состояния централизованной системы и разработку предложений по совершенствованию централизованной системы;

8) регулярное обновление версий антивирусного программного обеспечения и сигнатур антивирусных баз централизованной системы.

4.3. Субъект централизованной системы обеспечивает:

1) определение администратора (ов) антивирусной защиты;

2) эксплуатацию виртуального сервера администрирования субъекта централизованной системы;

3) установку антивирусного программного обеспечения на автоматизированных рабочих местах и серверах, контроль их функционирования;

4) контроль состояния антивирусной защиты информации на автоматизированном рабочем месте;

5) подключение автоматизированных рабочих мест и серверов к централизованной системе;

6) соблюдение и выполнение принятых координатором централизованной системы правовых актов, регламентирующих вопросы создания, организации работы и эксплуатации централизованной системы;

7) выполнение требований Регламента;

8) проведение проверок, связанных с активностью вредоносных компьютерных программ (вирусов) на серверах и автоматизированных рабочих местах.

4.4. Централизованный орган исполнительной власти Амурской области обеспечивает:

1) определение администратора (ов) антивирусной защиты;

2) подключение автоматизированных рабочих мест и серверов к централизованной системе;

3) соблюдение и выполнение принятых координатором централизованной системы правовых актов, регламентирующих вопросы создания, организации работы и эксплуатации централизованной системы;

4) выполнение требований Регламента;

5) проведение проверок, связанных с активностью вредоносных компьютерных программ (вирусов) на серверах и автоматизированных рабочих местах.

5. Права и обязанности администратора централизованной системы, администратора антивирусной защиты, пользователя централизованной системы

5.1. Администратор централизованной системы вправе:

1) запрашивать необходимую информацию у администраторов антивирусной защиты о работоспособности средств антивирусной защиты информации участников централизованной системы;

2) отказать в подключении к централизованной системе при невыполнении требований Регламента.

5.2. Администратор централизованной системы обязан:

1) соблюдать требования Регламента;

2) обеспечивать работоспособность главного и общего серверов администрирования централизованной системы;

3) проводить мониторинг работоспособности виртуальных серверов администрирования субъектов централизованной системы;

4) передать лицензию средства антивирусной защиты администратору антивирусной защиты.

5.3. Администратор антивирусной защиты субъекта централизованной системы вправе:

1) инициировать проведение служебных проверок по фактам заражения вредоносными компьютерными программами (вирусами) информационных ресурсов субъекта централизованной системы;

2) проводить расследования инцидентов, связанных с вирусной активностью.

5.4. Администратор антивирусной защиты субъекта централизованной системы обязан:

1) соблюдать требования Регламента;

2) обеспечивать работоспособность виртуального сервера администрирования субъекта централизованной системы;

3) осуществлять эксплуатацию виртуального сервера администрирования субъектов централизованной системы;

4) производить развёртывание антивирусного программного обеспечения на автоматизированных рабочих местах и серверах субъекта централизованной системы;

5) обеспечить подключение автоматизированных рабочих мест и серверов к виртуальному серверу администрирования субъекта централизованной системы;

6) осуществлять контроль состояния средств антивирусной защиты информации субъекта централизованной системы;

7) производить своевременное обновление версий, лицензий средств антивирусной защиты на автоматизированных рабочих местах и серверах субъекта централизованной системы;

8) по запросу администратора централизованной системы предоставлять информацию о состоянии средств антивирусной защиты;

9) обеспечить надежное хранение лицензии средства антивирусной защиты, исключающее возможность несанкционированного доступа;

10) не передавать и не распространять лицензию средства антивирусной защиты третьим лицам.

5.5. Администратор антивирусной защиты централизованного органа исполнительной власти Амурской области вправе:

1) инициировать проведение служебных проверок по фактам заражения вредоносными компьютерными программами (вирусами) информационных ресурсов централизованного органа исполнительной власти Амурской области;

2) проводить расследования инцидентов, связанных с вирусной активностью.

5.6. Администратор антивирусной защиты централизованного органа исполнительной власти Амурской области обязан:

1) соблюдать требования Регламента;

2) обеспечить подключение автоматизированных рабочих мест и серверов к главному серверу администрирования централизованной системы;

3) по запросу администратора централизованной системы предоставлять информацию о состоянии средств антивирусной защиты;

4) обеспечить надежное хранение лицензии средства антивирусной защиты, исключающее возможность несанкционированного доступа;

5) не передавать и не распространять лицензию средства антивирусной защиты третьим лицам.

5.7. Пользователь централизованной системы вправе:

1) запрашивать у администратора антивирусной защиты отчет о наличии вирусной активности на автоматизированном рабочем месте;

2) ознакомиться с правовыми актами, разработанными оператором централизованной системы.

5.8. Пользователь централизованной системы обязан:

1) соблюдать требования Регламента;

2) осуществлять контроль состояния средства антивирусной защиты информации на автоматизированном рабочем месте.