ПРАВИТЕЛЬСТВО РОСТОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

от 11.07.2019 № 465

г. Ростов-на-Дону

О централизованной системе антивирусной защиты информации

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

1. Установить, что обеспечение органов исполнительной власти Ростовской области антивирусной защитой информации осуществляется централизованно министерством информационных технологий и связи Ростовской области.

2. Утвердить Положение о централизованной системе антивирусной защиты информации в органах исполнительной власти Ростовской области согласно приложению.

3. Министерству информационных технологий и связи Ростовской области (Лопаткин Г.А.) обеспечить координацию централизованной системы антивирусной защиты информации.

4. Настоящее постановление вступает в силу со дня его официального опубликования.

5. Контроль за выполнением настоящего постановления возложить на заместителя Губернатора Ростовской области Рудого В.В.

Губернатор
Ростовской области — В.Ю. Голубев

Правительство Ростовской области
Управление документационного обеспечения

Постановление вносит
министерство информационных
технологий и связи
Ростовской области

Приложение
к постановлению
Правительства
Ростовской области
от 11.07.2019 № 465

ПОЛОЖЕНИЕ
о централизованной системе антивирусной защиты информации в органах исполнительной власти Ростовской области

1. Настоящее Положение определяет функциональное назначение централизованной системы антивирусной защиты информации в органах исполнительной власти Ростовской области (далее соответственно – централизованная система антивирусной защиты, органы исполнительной власти) и функциональные обязанности ее участников.

2. Централизованная система антивирусной защиты представляет собой совокупность методов и средств, объединяемых в единый комплекс, направленных на обеспечение защищенности информационных ресурсов органов исполнительной власти от воздействия вредоносных компьютерных программ (вирусов) и несанкционированных массовых почтовых рассылок, обнаружение вредоносных компьютерных программ (вирусов) и восстановление модифицированных такими программами (вирусами) файлов, а также предотвращение модификации информационных ресурсов органов исполнительной власти вредоносным кодом.

3. Для целей настоящего Положения используются следующие понятия:

координатор централизованной системы антивирусной защиты – министерство информационных технологий и связи Ростовской области;

оператор централизованной системы антивирусной защиты – государственное бюджетное учреждение Ростовской области «Региональный центр информационных систем», которое обеспечивает проведение централизованной антивирусной защиты информации в органах исполнительной власти с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы органов исполнительной власти, возникновения последствий факта заражения программного обеспечения вредоносными компьютерными программами (вирусами); а также устранение его последствий;

субъект централизованной системы антивирусной защиты – орган исполнительной власти, подключенный к централизованной системе антивирусной защиты;

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

сервер – специализированный компьютер для выполнения на нем сервисного программного обеспечения, используемый одновременно множеством пользователей;

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

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

вредоносная компьютерная программа (вирус) – вредоносное программное обеспечение, способное создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные сектора, а также распространять свои копии в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей системы антивирусной защиты информации или же приведения в негодность аппаратных комплексов компьютера;

локальная вычислительная сеть органа исполнительной власти – система, включающая в себя соединение автоматизированных рабочих мест и серверов с помощью соответствующего аппаратного и программного обеспечения в единую вычислительную сеть с целью совместного использования информационных ресурсов;

антивирусная защита – комплексная защита от вредоносных компьютерных программ (вирусов) и несанкционированного доступа к информационным ресурсам органов исполнительной власти, представляющая собой программный комплекс, созданный для контроля и управления автоматизированными рабочими местами;

администратор централизованной системы антивирусной защиты – должностное лицо оператора централизованной системы антивирусной защиты, определенное ответственным за эксплуатацию средств системы антивирусной защиты информации в органах исполнительной власти;

администратор антивирусной защиты – должностное лицо, определенное ответственным за проведение мероприятий по антивирусной защите информации в органе исполнительной власти;

пользователи централизованной системы антивирусной защиты – работники органов исполнительной власти, использующие в работе информационные ресурсы.

4. Централизованная система антивирусной защиты обеспечивает мониторинг работы и управление антивирусным программным обеспечением, используемым в локальных вычислительных сетях органов исполнительной власти, оптимизирует процесс распространения обновлений и мониторинга состояния антивирусной защиты информации.

5. Координатор централизованной системы антивирусной защиты обеспечивает:

методическое и организационное сопровождение централизованной системы антивирусной защиты;

принятие правовых актов, регламентирующих вопросы создания, организации работы и эксплуатации централизованной системы антивирусной защиты;

осуществление организационных мероприятий по антивирусной защите;

организацию планирования и оснащения органов исполнительной власти средствами антивирусной защиты информации.

6. Оператор централизованной системы антивирусной защиты обеспечивает:

утверждение Регламента работы централизованной системы антивирусной защиты информации (далее – Регламент);

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

определение администратора централизованной системы антивирусной защиты;

дистанционный контроль состояния антивирусной защиты информации на серверах администрирования субъектов централизованной системы антивирусной защиты и автоматизированных рабочих местах с автоматизированного рабочего места администратора централизованной системы антивирусной защиты;

анализ состояния и разработку предложений по совершенствованию централизованной системы антивирусной защиты;

регулярное обновление версий антивирусного программного обеспечения и сигнатур антивирусных баз централизованной системы антивирусной защиты.

Администратор централизованной системы антивирусной защиты осуществляет своевременную рассылку обновлений версий, лицензий антивирусного программного обеспечения и сигнатур антивирусных баз, мониторинг работоспособности централизованной системы антивирусной защиты в порядке, установленном Регламентом.

7. Субъект централизованной системы антивирусной защиты обеспечивает:

определение администратора антивирусной защиты;

установку и настройку сервера администрирования субъекта централизованной системы антивирусной защиты, а также антивирусного программного обеспечения на автоматизированных рабочих местах и серверах;

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

выполнение требований Регламента;

внесение предложений по совершенствованию централизованной системы антивирусной защиты;

участие в планировании мероприятий по антивирусной защите информации серверов администрирования субъекта централизованной системы антивирусной защиты и автоматизированных рабочих мест;

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

Руководитель органа исполнительной власти или иное уполномоченное лицо обеспечивает организацию работы в централизованной системе антивирусной защиты.

8. Технологическая инфраструктура централизованной системы антивирусной защиты состоит из следующих элементов:

сервер администрирования централизованной системы антивирусной защиты, развернутый на серверах координатора централизованной системы антивирусной защиты;

серверы администрирования субъектов централизованной системы антивирусной защиты;

автоматизированные рабочие места пользователей централизованной системы антивирусной защиты;

серверы субъектов централизованной системы антивирусной защиты.

9. Основными функциями сервера администрирования централизованной системы антивирусной защиты являются:

обновление сигнатур антивирусных баз централизованной системы антивирусной защиты;

отслеживание произошедших ситуаций наличия вредоносных компьютерных программ (вирусов) (далее – инцидент) в централизованной системе антивирусной защиты;

отслеживание режимов функционирования подчиненных серверов и автоматизированных рабочих мест;

формирование отчетов о состоянии централизованной системы антивирусной защиты;

контроль функционирования подчиненных серверов.

10. Основными функциями сервера администрирования субъекта централизованной системы антивирусной защиты являются:

поддержание актуальности сигнатур антивирусных баз автоматизированных рабочих мест;

отслеживание произошедших инцидентов на автоматизированных рабочих местах;

формирование отчетов о состоянии антивирусной защиты информации автоматизированных рабочих мест.

11. Основными функциями автоматизированного рабочего места и сервера являются:

защита от вредоносных компьютерных программ (вирусов);

обновление сигнатур антивирусных баз;

предотвращение и блокирование хакерских и сетевых атак.

12. Для подключения к централизованной системе антивирусной защиты необходимо наличие антивирусного программного обеспечения на всех стационарных и подключенных к локальной вычислительной сети органа исполнительной власти автоматизированных рабочих местах.

13. Отключение субъекта централизованной системы антивирусной защиты от централизованной системы антивирусной защиты осуществляется в случае ликвидации (реорганизации) субъекта централизованной системы антивирусной защиты.

В случае нарушения субъектом централизованной системы антивирусной защиты положений Регламента доступ к централизованной системе антивирусной защиты приостанавливается до устранения причин нарушения.

Начальник управления
документационного обеспечения
Правительства Ростовской области  Т.А. Родионченко