ПРАВИТЕЛЬСТВО
КЕМЕРОВСКОЙ ОБЛАСТИ - КУЗБАССА

П О С Т А Н О В Л Е Н И Е

от « 20 » сентября 2022 г. № 639
г. Кемерово

О централизованной системе антивирусной защиты информации

В целях реализации Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», обеспечения безопасности информационного обмена между органами государственной власти Кемеровской области – Кузбасса и органами местного самоуправления муниципальных образований Кемеровской области – Кузбасса Правительство Кемеровской области – Кузбасса п о с т а н о в л я е т:

1. Установить, что обеспечение безопасности информационного обмена между органами государственной власти Кемеровской области – Кузбасса, органами местного самоуправления муниципальных образований Кемеровской области – Кузбасса и подведомственными им государственными и муниципальными учреждениями (далее – подведомственные учреждения) осуществляется централизованно Министерством цифрового развития и связи Кузбасса.

2. Утвердить прилагаемое Положение о централизованной системе антивирусной защиты информации.

3. Министерству цифрового развития и связи Кузбасса обеспечить координацию взаимодействия участников централизованной системы антивирусной защиты информации.

4. Определить государственное казенное учреждение «Центр информационных технологий Кузбасса» ответственным за функционирование централизованной системы антивирусной защиты информации в соответствии с требованиями законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

5. Государственному казенному учреждению «Центр информационных технологий Кузбасса»:

5.1. Разработать план мероприятий («дорожную карту») по подключению органов государственной власти Кемеровской области – Кузбасса, органов местного самоуправления муниципальных образований Кемеровской области – Кузбасса и подведомственных им государственных и муниципальных учреждений к централизованной системе антивирусной защиты информации.

5.2. Обеспечить реализацию плана мероприятий («дорожной карты») по подключению органов государственной власти Кемеровской области – Кузбасса, органов местного самоуправления муниципальных образований Кемеровской области – Кузбасса и подведомственных им государственных и муниципальных учреждений к централизованной системе антивирусной защиты информации.

6. Органам государственной власти Кемеровской области – Кузбасса:

6.1. Обеспечить принятие мер по антивирусной защите информации в соответствии с Положением о централизованной системе антивирусной защиты информации.

6.2. Заключить с Министерством цифрового развития и связи Кузбасса соглашения об информационном взаимодействии.

6.3. Назначить уполномоченных лиц, ответственных за установку и настройку антивирусного программного обеспечения.

6.4. Не допускать приобретение антивирусного программного обеспечения для защиты автоматизированных рабочих мест и серверного оборудования, дублирующего функциональные возможности централизованной системы антивирусной защиты информации, со дня подключения к централизованной системе антивирусной защиты информации.

7. Рекомендовать органам местного самоуправления муниципальных образований Кемеровской области – Кузбасса, подведомственным им муниципальным учреждениям, государственным учреждениям Кемеровской области - Кузбасса:

7.1. Обеспечить принятие мер по антивирусной защите информации в соответствии с Положением о централизованной системе антивирусной защиты информации.

7.2. Для подключения к централизованной системе антивирусной защиты информации заключить с Министерством цифрового развития и связи Кузбасса соглашения об информационном взаимодействии.

7.3. Назначить уполномоченных лиц, ответственных за установку и настройку антивирусного программного обеспечения.

7.4. Не допускать приобретение антивирусного программного обеспечения для защиты автоматизированных рабочих мест и серверного оборудования, дублирующего функциональные возможности централизованной системы антивирусной защиты информации, со дня подключения к централизованной системе антивирусной защиты информации.

8. Настоящее постановление подлежит опубликованию на сайте «Электронный бюллетень Правительства Кемеровской области – Кузбасса».

9. Контроль за исполнением настоящего постановления возложить на заместителя председателя Правительства Кемеровской области - Кузбасса (по экономическому развитию и цифровизации) Ващенко С.Н.

Первый заместитель председателя Правительства Кемеровской области – Кузбасса – министр финансов Кузбасса

И.Ю. Малахов

УТВЕРЖДЕНО
постановлением Правительства
Кемеровской области – Кузбасса
от 20 сентября 2022 г. № 639

ПОЛОЖЕНИЕ
о централизованной системе антивирусной защиты информации

1. Общие положения

1.1. Настоящее Положение определяет функциональное назначение централизованной системы антивирусной защиты информации (далее - централизованная система антивирусной защиты) и порядок информационного взаимодействия ее участников.

1.2. Централизованная система антивирусной защиты представляет собой совокупность методов и средств, объединяемых в единый комплекс, направленных на обеспечение защищенности информационных ресурсов органов государственной власти Кемеровской области – Кузбасса, органов местного самоуправления муниципальных образований Кемеровской области – Кузбасса и подведомственных им государственных и муниципальных учреждений (далее – подведомственные учреждения) 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 государственной власти Кемеровской области – Кузбасса, органов местного самоуправления муниципальных образований Кемеровской области – Кузбасса и подведомственных им учреждений вредоносным кодом.

1.3. В настоящем Положении используются следующие основные понятия:

координатор централизованной системы антивирусной защиты (далее – координатор) - Министерство цифрового развития и связи Кузбасса;

вредоносная компьютерная программа (вирус) – вредоносное программное обеспечение, способное внедряться в код других программ, системные области памяти, загрузочные сектора, а также распространять свои копии в информационно-телекоммуникационной сети «Интернет» с целью нарушения работы программно-аппаратных комплексов;

субъект централизованной системы антивирусной защиты (далее – субъект) – органы государственной власти Кемеровской области – Кузбасса, органы местного самоуправления муниципальных образований Кемеровской области – Кузбасса и подведомственные им учреждения, подключенные к централизованной системе антивирусной защиты;

оператор централизованной системы антивирусной защиты (далее – оператор) - государственное казенное учреждение «Центр информационных технологий Кузбасса», которое обеспечивает проведение централизованной системы антивирусной защиты в субъектах с целью предотвращения несанкционированных вредоносных воздействий на их информационные ресурсы, определение и устранение последствий заражения программного обеспечения вредоносными компьютерными программами (вирусами);

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

пользователь централизованной системы антивирусной защиты (далее – пользователь) – сотрудники субъекта, использующие в работе информационные ресурсы;

автоматизированное рабочее место – персональный компьютер пользователя 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 – средство управления централизованной системой антивирусной защиты субъекта, позволяющее субъекту настраивать все компоненты системы антивирусной защиты информации субъекта;

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

локальная вычислительная сеть субъекта – 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;

администратор антивирусной защиты – должностное лицо, ответственное за установку и настройку антивирусного программного обеспечения в субъекте.

1.4. Централизованная система антивирусной защиты обеспечивает мониторинг работы и управление антивирусным программным обеспечением, используемым в локальных вычислительных сетях

субъектов, оптимизирует процесс распространения обновлений и мониторинга состояния антивирусной защиты информации.

2. Функции, полномочия и обязанности участников централизованной системы антивирусной защиты

2.1. Координатор:

2.1.1. Обеспечивает методическое и организационное сопровождение централизованной системы антивирусной защиты.

2.1.2. Обеспечивает утверждение регламента работы централизованной системы антивирусной защиты (далее – Регламент).

2.1.3. Обеспечивает принятие правовых актов, регламентирующих вопросы создания, организации работы и эксплуатации централизованной системы антивирусной защиты.

2.1.4. Обеспечивает осуществление организационных мероприятий по антивирусной защите.

2.2. Оператор:

2.2.1. Обеспечивает организацию планирования и оснащения субъектов средствами антивирусной защиты.

2.2.2. Определяет администратора централизованной системы антивирусной защиты.

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

2.2.4. Обеспечивает анализ состояния и разработку предложений по совершенствованию централизованной системы антивирусной защиты.

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

2.2.6. Приостанавливает доступ к централизованной системе антивирусной защиты в случае нарушения субъектом положений Регламента до устранения причин нарушения.

2.2.7. Отключает субъект от централизованной системы антивирусной защиты в случае ликвидации (реорганизации) субъекта.

2.2.8. Определяет время проведения регламентных работ по обновлению сигнатур антивирусных баз.

2.3. 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.

2.4. Субъект:

2.4.1. Заключает с координатором соглашение об информационном взаимодействии.

2.4.2. Определяет администратора антивирусной защиты.

2.4.3. Обеспечивает установку и настройку антивирусного программного обеспечения на автоматизированных рабочих местах и серверах.

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

2.4.5. Обеспечивает выполнение требований Регламента.

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

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

2.4.8. Имеет право вносить предложения оператору о необходимых изменениях в целях оптимизации централизованной системы антивирусной защиты.

2.5. Руководитель субъекта или иное уполномоченное лицо обеспечивает организацию работы в централизованной системе антивирусной защиты.

3. Функционирование централизованной системы антивирусной защиты

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

3.1.1. Сервер администрирования централизованной системы антивирусной защиты, развернутый на серверном оборудовании оператора.

3.1.2. Серверы администрирования субъектов.

3.1.3. Серверы субъектов.

3.1.4. Автоматизированные рабочие места пользователей.

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

3.2.1. Обновление сигнатур антивирусных баз централизованной системы антивирусной защиты.

3.2.2. Отслеживание произошедших ситуаций наличия вредоносных компьютерных программ (вирусов) (далее – инцидент) в централизованной системе антивирусной защиты.

3.2.3. Отслеживание режимов функционирования подчиненных серверов и автоматизированных рабочих мест.

3.2.4. Формирование отчетов о состоянии централизованной системы антивирусной защиты.

3.2.5. Контроль функционирования подчиненных серверов.

3.3. Основными функциями сервера администрирования субъекта являются:

3.3.1. Поддержание актуальности сигнатур антивирусных баз автоматизированных рабочих мест.

3.3.2. Отслеживание произошедших инцидентов на автоматизированных рабочих местах.

3.3.3. Формирование отчетов о состоянии антивирусной защиты информации автоматизированных рабочих мест.

3.4. Основными функциями автоматизированного рабочего места и сервера являются:

3.4.1. Защита от вредоносных компьютерных программ (вирусов).

3.4.2. Обновление сигнатур антивирусных баз.

3.4.3. Предотвращение и блокирование хакерских и сетевых атак.