МИНИСТЕРСТВО ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ АСТРАХАНСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

21.12.2021 № 14-П

О сервисе антивирусной защиты информации в единой мультисервисной телекоммуникационной сети Правительства Астраханской области

В соответствии с распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области», а также в целях совершенствования системы защиты информации в единой мультисервисной сети Правительства Астраханской области министерство государственного управления, информационных технологий и связи Астраханской области ПОСТАНОВЛЯЕТ:

1. Утвердить положение о сервисе антивирусной защиты информации в единой мультисервисной телекоммуникационной сети Правительства Астраханской области согласно приложению.

2. Отделу информационной безопасности министерства обеспечить размещение текста настоящего постановления на официальном сайте министерства в информационно-телекоммуникационной сети «Интернет» по адресу http://mingos.astrobl.ru/.

3. Отделу нормативно-правового обеспечения проектов министерства в семидневный срок направить его копию:

– в прокуратуру Астраханской области и Управление Министерства юстиции Российской Федерации по Астраханской области;

– поставщикам справочно-правовых систем «КонсультантПлюс», ЗАО «ТЕЛЕКОМ-СКИФ» и «ГАРАНТ» ЗАО НПП «Астрахань-Гарант-Сервис».

4. Постановление вступает в силу со дня его опубликования.

И.о. министра А.В. Набутовский

УТВЕРЖДЕНО
постановлением министерства
государственного управления,
информационных технологий и
связи Астраханской области
от 14.12.2021 № 11-Т

Положение о сервисе антивирусной защиты информации в единой мультисервисной телекоммуникационной сети Правительства Астраханской области

1. Общие положения

1.1. Положение о сервисе антивирусной защиты информации в единой мультисервисной телекоммуникационной сети Правительства Астраханской области (далее – Положение) разработано в соответствии с распоряжением Правительства Астраханской области от 18.09.2013 № 424-Пр «О единой мультисервисной телекоммуникационной сети Правительства Астраханской области», а также в целях совершенствования системы защиты информации в единой мультисервисной телекоммуникационной сети Правительства Астраханской области.

1.2. Приведенные в данном разделе термины и определения применяются в настоящем Положении в следующих значениях:

АВЗИ – антивирусная защита информации;

АРМ – автоматизированное рабочее место;

вредоносное программное обеспечение – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы;

ЕМТС – единая мультисервисная телекоммуникационная сеть Правительства Астраханской области;

координатор сервиса АВЗИ ЕМТС – министерство государственного управления, информационных технологий и связи Астраханской области;

ИОГВ АО – исполнительные органы государственной власти Астраханской области;

ОМСУ АО – органы местного самоуправления муниципальных образований Астраханской области;

ведомства – ИОГВ АО и подведомственные им государственные учреждения, ОМСУ АО и подведомственные им муниципальные учреждения;

политика АВЗИ ЕМТС – набор требований к реализации антивирусной защиты информации, осуществляемый в соответствии с постановлением министерства государственного управления, информационных технологий и связи Астраханской области от 20.04.2021 № 4-П «О работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области», путем настройки параметров работы антивирусного программного обеспечения;

пользователи ЕМТС – работники ведомств, подключенных к ЕМТС;

сервис АВЗИ ЕМТС – сервис антивирусной защиты информации единой мультисервисной телекоммуникационной сети Правительства Астраханской области;

сервер администрирования АВЗИ ЕМТС - средство централизованного управления сервиса АВЗИ ЕМТС, позволяющее настраивать все его компоненты;

технический оператор сервиса АВЗИ ЕМТС – государственное бюджетное учреждение Астраханской области «Инфраструктурный центр электронного правительства»;

администратор сегмента ЕМТС – работник из числа пользователей ЕМТС, ответственный за антивирусную защиту информации, назначенный администратором безопасности информации.

1.3. В Положении определены сервис АВЗИ ЕМТС, единый порядок оснащения средствами антивирусной защиты, обновления баз данных и их эксплуатации.

1.4. Сервис АВЗИ ЕМТС является частью системы защиты информации в ЕМТС и предназначен для предотвращения заражения и минимизации воздействия вредоносных компьютерных программ (вирусов) на информационно-вычислительные ресурсы ведомств, подключенных к ЕМТС.

1.5. Антивирусная защита информации в ведомствах осуществляется посредством применения организационных мероприятий, административных мер и программных средств АВЗИ.

1.6. Функционирование сервиса АВЗИ ЕМТС осуществляется в рамках работ по созданию и развитию системы защиты информации в ведомствах, подключенных к ЕМТС.

2. Сервис АВЗИ ЕМТС

2.1. Сервис АВЗИ ЕМТС является комплексной системой, состоящей из совокупности организационных, правовых и программно-аппаратных мер и средств, направленных на обеспечение эффективной антивирусной защиты информации в ведомствах, подключенных к ЕМТС. Комплексность системы антивирусной защиты достигается контролем информационных потоков, протекающих в ЕМТС, и согласованием между собой разнородных методов и средств, обеспечивающих антивирусную защиту всех элементов ЕМТС.

2.2. Координатор сервиса АВЗИ ЕМТС осуществляет:

- общее руководство сервисом АВЗИ ЕМТС;

- разработку проектов нормативных правовых актов, регламентирующих функционирование сервиса АВЗИ ЕМТС;

- планирование мероприятий по антивирусной защите;

- контроль состояния антивирусной защиты информации в ведомствах, подключенных к ЕМТС, в рамках своих полномочий, определенных постановлением Правительства Астраханской области от 20.03.2020 № 108-П

«О министерстве государственного управления, информационных технологий и связи Астраханской области».

2.3. Технический оператор сервиса АВЗИ ЕМТС обеспечивает:

- практическую реализацию мероприятий по обеспечению функционирования и обновления программного обеспечения сервиса АВЗИ ЕМТС;

- непрерывное функционирование центра администрирования АВЗИ ЕМТС;

- применение и соблюдение политики АВЗИ ЕМТС всеми средствами антивирусной защиты, управляемыми сервером администрирования АВЗИ ЕМТС;

- закупку прав использования (лицензий) средств АВЗИ для функционирования сервиса АВЗИ ЕМТС;

- оснащение сервиса АВЗИ ЕМТС, средствами антивирусной защиты;

- автоматизированный учет средств АВЗИ;

- антивирусную защиту почтовых сообщений в ЕМТС.

2.4. При организации сервиса АВЗИ ЕМТС используется специализированное программное обеспечение, допускающее дистанционное управление антивирусным программным обеспечением техническим оператором сервиса АВЗИ ЕМТС.

2.5. Администраторы сегмента ЕМТС обеспечивают и контролируют в ведомствах, подключенных к ЕМТС:

- исполнение настоящего Положения;

- ликвидацию активных угроз безопасности (вредоносное программное обеспечение, сетевые атаки) по мере возникновения этих угроз;

- предварительную проверку устанавливаемого программного обеспечения, использование доверенных источников при получении программного обеспечения;

- своевременное обновление системного и прикладного программного обеспечения с целью устранения имеющихся в нем уязвимостей;

- отключение неиспользуемых сервисов и приложений;

- мониторинг и реагирование на информацию разработчиков систем и прикладного программного обеспечения об обнаруженных ошибках и уязвимостях;

- анализ и обеспечение хранения не менее 1 месяца информации (журналов) о событиях в системном и прикладном программном обеспечении, средствах защиты информации и сетевых устройств.

2.6. Ведомства, подключенные к ЕМТС, вправе усилить АВЗИ своих информационных ресурсов, направив официальный запрос техническому оператору сервиса АВЗИ ЕМТС о внесении изменений в политику сервиса АВЗИ, распространяемую на данное ведомство.

2.7. Технический оператор сервиса АВЗИ ЕМТС вправе предоставить полномочия самостоятельного управления политикой АВЗИ ведомству, подключенному к ЕМТС, на основании направленной координатору сервиса

АВЗИ заявки, включающей обоснование необходимости самостоятельного управления, а также сведений об ответственных за реализацию политики АВЗИ в ведомстве.

2.8. Политика АВЗИ, централизованно распространяемая техническим оператором сервиса АВЗИ ЕМТС, или собственная политика АВЗИ ведомств должна обеспечивать:

- централизованное управление средствами АВЗИ и обновлениями антивирусных баз;

- периодическое, не реже 1 раза в сутки в рабочие дни, обновление антивирусных баз;

- получение уведомлений о необходимости обновлений;

- полную антивирусную проверку информационных систем и АРМ, проводимую периодически, не реже одного раза в неделю (сканирование);

- обязательный антивирусный контроль любой информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, сообщения электронной почты), получаемой и передаваемой по телекоммуникационным каналам связи, на съемных носителях, а также при запуске, открытии и исполнении;

- оповещение об обнаружении вредоносного программного обеспечения.

2.9. В случае самостоятельного управления политикой АВЗИ ЕМТС ведомство, подключенное к ЕМТС, несет ответственность за неисполнение (ненадлежащее исполнение) требований политики сервиса АВЗИ в рамках реализации мер по АВЗИ.

2.10.Технический оператор сервиса АВЗИ ЕМТС несет ответственность за неисполнение (ненадлежащее исполнение) возложенных на него обязанностей в рамках реализации мер по АВЗИ.

2.11.Пользователи ЕМТС несут ответственность за обеспечение установленных норм АВЗИ на своих АРМ.

2.12.Пользователю ЕМТС запрещается отключать антивирусное программное обеспечение.

3. Порядок установки и обновления баз данных средств АВЗИ

3.1. АРМ, используемые в ведомствах, подключенных к ЕМТС, в обязательном порядке оснащаются средствами АВЗИ.

3.2. К использованию в государственных информационных системах, а также информационных системах, обрабатывающих информацию ограниченного доступа, в том числе персональные данные, допускаются только сертифицированные Федеральной службой по техническому и экспортному контролю антивирусные средства защиты.

3.3. Установка антивирусного программного обеспечения осуществляется в автоматическом режиме при предоставлении доступа к ресурсам ЕМТС.

3.4. Установка антивирусного программного обеспечения для информационных ресурсов, не имеющих подключения к ЕМТС, осуществляется администратором сегмента ЕМТС самостоятельно с использованием предоставляемого техническим оператором сервиса АВЗИ ЕМТС установочного комплекта АВЗИ.

3.5. Своевременное обновление баз данных средств АВЗИ информации является неотъемлемой частью обеспечения эффективной антивирусной защиты информации. Обновления антивирусных баз и активация лицензий антивирусного программного обеспечения осуществляются техническим оператором сервиса АВЗИ ЕМТС.

3.6. Обновление баз данных средств АВЗИ осуществляется централизованно через серверы администрирования техническим оператором сервиса АВЗИ ЕМТС ежедневно, а для автоматизированных рабочих мест, не имеющих подключения к ЕМТС, – еженедельно.

4. Порядок информирования о вирусной активности

4.1. Своевременное информирование пользователей ЕМТС о вирусной активности является составной частью системы АВЗИ. Информирование пользователей ЕМТС производится техническим оператором АВЗИ ЕМТС.

4.2. При возникновении вирусной активности технический оператор сервиса АВЗИ ЕМТС организует почтовую рассылку с рекомендациями по предотвращению заражений средств вычислительной техники вредоносным программным обеспечением.

5. Действия при обнаружении вредоносного программного обеспечения

5.1. В соответствии с порядком реагирования на компьютерные инциденты в единой мультисервисной телекоммуникационной сети Правительства Астраханской области, утвержденного постановлением министерства государственного управления, информационных технологий и связи Астраханской области от 20.04.2021 № 4-П «О работе в единой мультисервисной телекоммуникационной сети Правительства Астраханской области» при выявлении пользователем ЕМТС или администратором сегмента ЕМТС признаков функционирования вредоносного программного обеспечения, необходимо:

– сообщить о данном факте с указанием внутреннего ip-адреса зараженного АРМ техническому оператору сервиса АВЗИ ЕМТС;

– отключить зараженное АРМ ото всех средств коммуникации и сети электропитания;

– зафиксировать точную дату и время отключения зараженного АРМ;

– проинформировать технического оператора сервиса АВЗИ ЕМТС о проведенных мероприятиях и ждать дальнейших инструкций.

5.2. В случае обнаружения вредоносного программного обеспечения при входном контроле машинных носителей информации, файлов или

почтовых сообщений, поступивших в ведомства, пользователь ЕМТС обязан прекратить процесс приема-передачи информации. Если входящая информация (носитель) поступила из внутренней сети ведомств, подключенных к ЕМТС, пользователь ЕМТС обязан сообщить о факте обнаружения вредоносного программного обеспечения техническому оператору сервиса АВЗИ ЕМТС по телефону и электронной почте.

5.3. Техническому оператору сервиса АВЗИ ЕМТС при получении информации факте обнаружения вредоносного программного обеспечения в течение 24 часов необходимо проинформировать федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования ГосСОПКА (УФСБ России по Астраханской области, телефон: 44-36-88, факс: 44-39-76). В сообщении уведомить о факте обнаружения вредоносного программного обеспечения и месте его возникновения, предоставить контактный номер телефона для организации последующего взаимодействия.