Приложение № 2

к приказу руководителя Департамента информатизации и связи Забайкальского края от \_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_ г. № \_\_\_\_\_

**Инструкция по организации антивирусной защиты автоматизированной системы Департамента информатизации и связи Забайкальского края**

**1 Общие положения**

1.1 Инструкция по организации антивирусной защиты информационных систем Департамента информатизации и связи Забайкальского края (далее - Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г. №Пр-1895.

1.2 Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в корпоративной сети передачи данных государственных органов Забайкальского края (далее – КСПД) с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы и персональные данные исполнительных органов государственной власти Забайкальского края и возникновения фактов заражения программного обеспечения (далее - ПО) сетевого оборудования и автоматизированных рабочих мест исполнителей компьютерными вирусами.

1.3 В настоящей Инструкции использованы следующие термины и определения:

**Антивирусное ПО** – набор программ для обнаружения компьютерных вирусов и других вредоносных программ и лечения инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом.

**Антивирусные базы** – файлы, используемые антивирусным ПО при поиске вредоносных программ, периодически обновляемые разработчиком антивирусного ПО.

**Антивирусный контроль** – проверка информации (файла, сообщения и т.п.) на предмет наличия вредоносных программ.

**Вредоносная программа** – компьютерная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информационные ресурсы.

**Защищаемый компьютер** – электронно-вычислительная машина (персональный компьютер или сервер), используемая для обработки данных.

**Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Пользователь** – работник исполнительного органа государственной власти Забайкальского края (далее – ИОГВ) или другое лицо, использующее в работе средства электронно-вычислительной техники ИОГВ, назначенный приказом Руководителя ИОГВ.

**Съемный носитель информации** – носитель информации, предназначенный для ее автономного хранения и независимого от места записи использования (отторгаемые жесткие магнитные диски, флэш-память, CD, DVD, дискеты и др.).

**Участник КСПД** – исполнительный орган государственной власти Забайкальского края, или иная организация (учреждение, предприятие), имеющее подключение к ресурсам корпоративной сети передачи данных государственных органов Забайкальского края в соответствии со своими правами и полномочиями.

1.4 Требования настоящей Инструкции обязательны для выполнения всеми сотрудниками ИОГВ, ведущими обработку конфиденциальной информации, персональных данных и другой информации с применением средств вычислительной техники.

1.5 Общее и методическое руководство обеспечением антивирусной защиты информационных систем и информационных систем персональных данных в КСПД осуществляется отделом технической политики и защиты информации (далее – ОТПЗИ).

В исполнительных органах государственной власти Забайкальского края руководство антивирусной защитой осуществляют должностные лица ответственные за обеспечение безопасности информации, определенные приказами руководителей участников КСПД.

1.6 Пользователь отвечает за обеспечение устойчивой работоспособности и информационной безопасности вверенного ему объекта вычислительной техники при работе в информационных системах и при обработке персональных данных.

1.7 Техническое обслуживание средств вычислительной техники, уборка помещения и т.п. проводятся под контролем пользователя либо другого штатного сотрудника ИОГВ.

**2. Установка антивирусного ПО**

2.1 Установку антивирусного ПО производят работники ИОГВ отвечающие за работу информационных систем и вычислительной техники (системные администраторы, администраторы информационных систем, а где их нету – сотрудники исполняющие их обязанности и обладающие соответствующими знаниями и навыками).

2.2 В ИОГВ должно использоваться только лицензионное антивирусное ПО, рекомендованное к применению ОТПЗИ Департамента информатизации и связи Забайкальского края.

2.3 Установка антивирусного ПО производится индивидуально на каждый защищаемый компьютер с обязательным предохранением настроек от изменения паролем.

2.4 Пользователям запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного ПО.

2.5 Ярлык для запуска антивирусного ПО должен быть вынесен на "Рабочий стол" операционной системы.

2.6 В случае необходимости использования антивирусных средств, не вошедших в перечень рекомендованных, их применение необходимо согласовать с ОТПЗИ Департамента информатизации и связи Забайкальского края.

**3 Порядок обновления антивирусных баз**

3.1 Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети ИОГВ, имеющей подключение к КСПД, должна осуществляться ежедневно в автоматическом режиме с сервера управления антивирусной защитой корпоративной сети передачи данных органов власти Забайкальского края или с сервера обновлений ЗАО «Лаборатория Касперского через единую защищенную точку доступа в сеть «Интернет» (по рабочим дням).

3.2 Обновление антивирусных баз на защищаемых компьютерах, не подключенных к локальной сети ИОГВ, должно осуществляться с использованием учтенных съемных носителей информации, в обязательном порядке проверяемых антивирусным ПО перед их использованием или принудительным подключением к локальной сети ИОГВ.

3.3 Проверка критических областей защищаемых компьютеров, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

3.4 Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети ИОГВ, контролируется пользователем самостоятельно ежедневно и в случае нарушения пользователь должен не принимать никаких мер и срочно сообщить ответственному за обеспечение безопасности информации ИОГВ, который в свою очередь должен официально сообщить о данном инциденте информационной безопасности в ОТПЗИ Департамента информатизации и связи Забайкальского края.

**4 Требования к проведению антивирусного контроля**

4.1 Пользователь осуществляет контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств.

4.2 Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, сообщения электронной почты и т.д.), получаемая и передаваемая по телекоммуникационным каналам, а также данные на съемных носителях информации. Контроль входящей и исходящей информации на защищаемых компьютерах должен осуществляться непрерывно посредством постоянно работающего компонента антивирусного ПО («монитора»).

4.3 Все программное обеспечение, устанавливаемое на защищаемые компьютеры, должно предварительно проверяться на наличие вредоносных программ.

4.4 Полная проверка сетевых ресурсов и рабочих станций на наличие компьютерных вирусов производится еженедельно, по четвергам.

4.5 Внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера должен выполняться:

– сразу после установки или изменения ПО;

– после подключения автономного компьютера к локальной сети;

– при возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках, сбоях и т.п.).

4.6 В сомнительных случаях для определения факта наличия или отсутствия вредоносных программ к проверке необходимо привлечь специалистов ОТПЗИ Департамента информатизации и связи Забайкальского края.

Администратор безопасности информации ИОГВ обязан регулярно докладывать ответственному за обеспечение безопасности информации ИОГВ о результатах периодической проверки состояния антивирусной защиты.

**5 Действия пользователей при обнаружении вредоносных программ**

5.1 В случае обнаружения при проведении антивирусной проверки вредоносных программ пользователи обязаны:

– приостановить все операции, связанные с обработкой файлов на защищаемом компьютере;

– немедленно поставить в известность о факте обнаружения вредоносных программ ответственного за обеспечение безопасности информации ИОГВ, владельцев зараженных или поврежденных вредоносными программами файлов, а также смежные подразделения, использующие эти файлы в работе;

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– после доклада в ОТПЗИ Департамента информатизации и связи Забайкальского края, по разрешению начальника отдела, провести лечение зараженных файлов (при необходимости привлечь специалистов ОТПЗИ Департамента информатизации и связи Забайкальского края);

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на отторгаемом носителе в отдел технической политики и защиты информации для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

- по факту обнаружения зараженных вирусом файлов составить служебную записку в ОТПЗИ Департамента информатизации и связи Забайкальского края, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

**6 Ответственность за выполнение требований Инструкции**

6.1 Ответственность за организацию антивирусной защиты информации на компьютерах, эксплуатируемых подчиненными работниками, и их ознакомление с Инструкцией несет ответственный за обеспечение безопасности информации ИОГВ.

6.2 Ответственность за соблюдение требований Инструкции на своих рабочих местах несут пользователи.

6.3 Ответственность за своевременное обновление антивирусных баз и получение новых лицензионных ключей при истечении их срока действия несет лицо, ответственное за получение, распределение и установку программного обеспечения в ИОГВ.

6.4 За нарушение требований Инструкции пользователи несут дисциплинарную ответственность в соответствии с действующим законодательством.

Приложение: Порядок настройки антивируса Касперского