Приложение к приказу
от «08» апреля 2025 г.
№ 105-ОД

Политика
Государственного бюджетного учреждения города Москвы «Жилищник района Коньково» (ГБУ «Жилищник района Коньково») в отношении антивирусной защиты информационных систем и ресурсов

Настоящая политика антивирусной защиты информационных систем и ресурсов (далее – Политика) устанавливает общие правила и требования по обеспечению защиты информационных систем и ресурсов, ИТ-инфраструктуры, создание, развитие (модернизацию), эксплуатацию которых осуществляет Государственное бюджетное учреждение города Москвы «Жилищник района Коньково» (ГБУ «Жилищник района Коньково») от вредоносных программ (программного обеспечения).

1. Термины и определения

В настоящей Политике используются следующие основные термины и определения:

Администратор – лицо, назначаемое ответственным за управление (администрирование) системой защиты информации в ИСиР и/или ИТ-инфраструктуре распорядительным документом префектуры.

Антивирусная защита – защита информации и компонентов ИСиР или ИТ-инфраструктуры от вредоносных программ (обнаружение вредоносных программ, блокирование, изолирование объектов, попавших под воздействие вредоносных программ, удаление вредоносных программ из таких объектов).

База сигнатур – база данных признаков вредоносных программ (сигнатуры) – составная часть средства антивирусной защиты, содержащая информацию о вредоносных программах, используемая средством антивирусной защиты для обнаружения вредоносных программ и их обработки.

Вредоносная программа (программное обеспечение, вирус) – компьютерная программа либо иная компьютерная информация, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

ИСиР – информационные системы и ресурсы, создание, развитие (модернизацию), эксплуатацию которых осуществляет префектура.

ИТ-инфраструктура – совокупность программных и аппаратных средств, в том числе автоматизированных рабочих мест, с использованием которых осуществляется реализация возложенных на префектуру

государственных функций и полномочий, а также доступ к ИСиР города Москвы.

Комплексная система антивирусной защиты (КСАЗ) – иерархия средств антивирусной защиты, централизованное управление которой обеспечивает ГКУ «Инфогород».

Консоль централизованного управления – программное обеспечение, предназначенное для централизованного решения основных задач по управлению, настройке и обслуживанию средств антивирусной защиты.

Объект воздействия – информация, обрабатываемая в ИСиР, программное обеспечение, автоматизированные рабочие места, серверы, виртуальная инфраструктура, телекоммуникационное оборудование, средства защиты информации, съемные машинные носители информации и другие компоненты ИСиР, на нарушение штатной работы которых направлено воздействие вредоносных программ.

Пользователь – лицо, участвующее в функционировании ИСиР или использующее результаты ее функционирования и являющееся обладателем учетной записи в ИСиР.

Сигнатура вредоносной программы – характерные признаки вредоносной программы, используемые для ее обнаружения.

2. Организация антивирусной защиты

2.1. Администраторы обеспечивают организацию антивирусной защиты (установку, настройку, обновление баз сигнатур и иных модулей средств антивирусной защиты до актуальной версии), обеспечивающую обнаружение
и устранение вредоносных программ и последствий от их функционирования.

2.2. Администраторы обеспечивают организацию автоматических процессов по обновлению сигнатур вредоносных программ и необходимых проверок по поиску вредоносных программ посредством консоли централизованного управления КСАЗ.

Исключение составляют ИСиР и/или ИТ-инфраструктуры с ограниченным сетевым взаимодействием, или имеющие иные ограничения для автоматизированных рабочих мест (далее – АРМ) пользователей или серверов ИСиР и/или ИТ-инфраструктуры, не позволяющие подключить средства антивирусной защиты к КСАЗ. В этом случае порядок по обновлению сигнатур вредоносных программ и необходимых проверок по поиску вредоносных программ определяется в отношении конкретной ИСиР и/или ИТ-инфраструктуры в эксплуатационной документации и документах, определяющих правила процедуры, реализуемые для обеспечения защиты информации в ИСиР и/или ИТ-инфраструктуре в ходе ее эксплуатации (далее - организационно-распорядительная документация).

2.3. Допускается применение только лицензионных средств антивирусной защиты, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности

информации.

2.4. Средства антивирусной защиты должны функционировать непрерывно (при условии функционирования технических средств, на которых установлены) в круглосуточном режиме и обеспечивать:

- обнаружение различных видов вредоносных программ и реагирование на обнаружение таких программ;
- возможность блокирования доступа к вредоносным программам на отчуждаемых носителях информации в случае обнаружения фактов вирусного заражения объектов воздействия или активизации вредоносных программ;
- восстановление зараженных объектов воздействия;
- возможность автоматического получения обновлений баз сигнатур;
- возможность централизованного принудительного обновления;
- возможность централизованного управления и мониторинга с одного рабочего места;
- возможность оповещения о происходящих событиях.

2.5. Установка средств антивирусной защиты должна осуществляться в соответствии с эксплуатационной документацией, поставляемой вместе с такими средствами.

2.6. Обязательному антивирусному контролю подлежат:

- файлы загрузки операционной системы;
- программные средства, исполняемые файлы;
- файлы любых форматов, поступающие в системное программное обеспечение компонентов, входящих в состав ИСиР и/или ИТ-инфраструктуры, по каналам передачи данных или с использованием съемных носителей информации;
- файлы любых форматов, записываемые на съемный носитель информации;
- дистрибутивы системного и прикладного программного обеспечения.

2.7. Контроль отсутствия вредоносных программ должен проводиться в обязательном порядке в следующих случаях:

- для файлов загрузки – при загрузке операционной системы;
- для файлов системного и прикладного программного обеспечения, исполняемых файлов – в автоматическом режиме в период сеанса работы;
- для файлов, поступивших в системное программное обеспечение компонентов, входящих в состав ИСиР и/или ИТ-инфраструктуры, по каналам передачи данных или с использованием съемных носителей информации – в автоматическом режиме до открытия информации (запуска исполняемых файлов);
- для файлов на съемных носителях – при подключении съемного носителя к техническому средству;
- для исходящих файлов – непосредственно перед их записью на съемный носитель информации;
- для устанавливаемого (изменяемого) программного обеспечения – непосредственно перед установкой;

- для машинных носителей информации, стационарно установленных в корпус средств вычислительной техники (например, накопители на жестких дисках) – не реже одного раза в неделю.

2.8. Обновление баз сигнатур осуществляется только посредством КСАЗ, за исключением ИСиР и/или ИТ-инфраструктуры с ограниченным сетевым взаимодействием, или иными ограничениями АРМ и серверов, не позволяющими подключить средства антивирусной защиты к КСАЗ. В этом случае порядок обновления баз сигнатур определяется в отношении конкретной ИСиР и/или ИТ-инфраструктуры в эксплуатационной и организационно-распорядительной документации.

2.9. Обновление баз сигнатур проводится не реже одного раза в сутки (при их наличии). В случае сбоя автоматического обновления, обновление баз сигнатур должно производиться вручную с той же периодичностью.

2.10. Обновление модулей средств антивирусной защиты, направленных на устранение уязвимостей, на добавление новых функции или улучшение существующих, должно производиться с периодичностью не реже
1 раза в месяц.

2.11. Для всех применяемых средств антивирусной защиты должно вестись протоколирование событий безопасности.

2.12. Срок хранения журналов регистрации событий безопасности должен составлять не менее 1 года, журналы регистрации событий безопасности должны быть в оперативном доступе не менее 3 месяцев.

2.13. Журналы регистрации событий безопасности средств антивирусной защиты должны передаваться в КСАЗ и быть доступны для просмотра через консоль централизованного управления.

Исключение составляют ИСиР и/или ИТ-инфраструктура с ограниченным сетевым взаимодействием, или имеющие иные ограничения для АРМ пользователей или серверов ИСиР и/или ИТ-инфраструктуры, не позволяющие подключить средства антивирусной защиты к КСАЗ. В этом случае порядок ведения и хранения журналов регистрации событий определяется в отношении конкретной ИСиР и/или ИТ-инфраструктуры в эксплуатационной и организационно-распорядительной документации с учетом требований настоящей Политики.

2.14. Частные правила, требования и последовательность действий по обеспечению защиты от вредоносных программ описываются в проектной, эксплуатационной документации на ИСиР и/или ИТ-инфраструктуры, а также в организационно-распорядительной документации, разработанных на основании настоящей Политики при создании (развитии, модернизации) системы (подсистемы) защиты информации ИСиР и/или ИТ-инфраструктуры.

3. Действия в случае обнаружения или подозрения на наличие вредоносных программ

3.1. При обнаружении вредоносных программ Администраторы

обеспечивают выполнение следующих мероприятий:

- анализ возможности и(или) необходимости дальнейшего использования объектов, попавших под воздействие (зараженных) вредоносной программой (вирусом);
- информирование руководства;
- предотвращение дальнейшего заражения вирусом ИСиР и/или ИТ-инфраструктуры;
- обеспечение (при необходимости) технически максимально возможной изоляции источников заражения вирусом на сетевом или физическом уровне

до завершения работ по устранению вредоносных программ и последствий от их функционирования;

- устранение вредоносных программ и ликвидация последствий их функционирования;
- восстановление зараженных вирусом объектов;
- выявление причин заражения вирусом;
- устранение возможности повторного заражения вирусом в будущем.

3.2. При фиксировании массового заражения вирусом АРМ пользователей и (или) компонентов ИСиР и/или ИТ-инфраструктуры, влияющих на работоспособность (функционирование) ИСиР и/или ИТ-инфраструктуры, Администраторы обеспечивают незамедлительное уведомление о данном факте Департамента информационных технологий города Москвы в порядке, определенном распоряжением департамент от 03.10.2022 № 64-16-482/22 «Об утверждении порядка предоставления сведений об инцидентах информационной безопасности».

4. Контроль

4.1. Администраторы на регулярной основе, но не реже, чем один раз в 6 месяцев проводят анализ статистических данных по работе средств антивирусной защиты на соответствие установленным требованиям, в том числе в настоящей Политике: информацию о количестве обнаруженных вредоносных программ, примененных к ним действий и их результатов, об ошибках работы средств антивирусной защиты, информацию об удалении средств антивирусной защиты, информацию об актуальности используемых средств антивирусной защиты, баз сигнатур, статистические данные о наличии/отсутствии средств антивирусной защиты на компонентах ИСиР и/или ИТ-инфраструктуры. По результатам анализа принимаются меры по устранению выявленных нарушений.

5. Ответственность

Администраторы несут персональную ответственность за соблюдение требований настоящей Политики.