КГУ «Управление архитектуры и градостроительства города Алматы»

УТВЕРЖДЕНО

Начальник Управления архитектуры и градостроительства города Алматы

_____ Ахмеджанов А. Т.

«14» января 2019 г.

М. П.

Правила организации антивирусного контроля Информационной системы «3D автоматизированная геоинформационная система города Алматы» 3DГЕО.СМИБ.ПР.11.r10.17

г. Алматы
2019 г.

1. Область применения

Целью настоящего документа является описание правил организации антивирусного контроля, и определение порядка действий ответственных сотрудников Организации, а также определение ответственности при проведении этих мероприятий или нарушении требований настоящего Документа.

Настоящий документ обязателен для исполнения в рамках проекта ИС.

2. Нормативные ссылки

Настоящий документ содержит указания к практическому исполнению требований изложенных в нормативных документах согласно п. 3 Нормативные ссылки действующей Политики информационной безопасности.

3. Термины, определения и сокращения

В настоящем документе используются термины и сокращения, принятые в действующей Политике информационной безопасности.

4. Общие положения

В настоящем документе описаны меры по обнаружению, предотвращению проникновения и восстановлению после проникновения вредоносного кода, а также установлены требования к обеспечению соответствующего оповещения пользователей.

5. Меры защиты от вредоносного кода

Защита от вредоносного программного обеспечения основывается на понимании требований безопасности, соответствующих мерах контроля доступа к системам и надлежащем управлении изменениями.

В Организации применяются следующие мероприятия по управлению информационной безопасностью в отношении вредоносного кода:

a) требуется соблюдение лицензионных соглашений и установлен запрет на использование неавторизованного программного обеспечения;

b) настоящий документ определяет механизмы защиты от рисков, связанных с получением файлов и программного обеспечения из внешних сетей, через внешние сети или из любой другой среды;

c) в рамках аудита проводится инвентаризация программного обеспечения и данных систем, поддерживающих критические бизнес-

процессы. Все случаи выявления любых неавторизованных или измененных файлов в системе проводятся работы по определению причин инцидента ИБ;

d) установка и регулярное обновление антивирусного программного обеспечения для обнаружения и сканирования компьютеров и носителей информации, запускаемого в случае необходимости в качестве превентивной меры или рутинной процедуры. Выполняются следующие проверки:

1) проверка всех файлов на носителях информации сомнительного или неавторизованного происхождения, или файлов, полученных из общедоступных сетей, на наличие вирусов перед работой с этими файлами;

2) проверка любых вложений электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения до их использования. Эта проверка выполняется в двух точках, при входе в сеть организации и на рабочих станциях.

3) поверка веб-страниц на наличие вредоносного программного обеспечения;

a) управленческие процедуры и обязанности, связанные с защитой от вирусов, обучение применению этих процедур, а также вопросы оповещения и восстановления после вирусных атак;

b) планы по обеспечению непрерывности бизнеса учитывают работы в части восстановления после вирусных атак, включая все необходимые мероприятия по резервированию и восстановлению данных и программного обеспечения;

c) ответственный за обеспечение ИБ ведет сбор информации, таких как подписка на почтовые списки и/или проверка веб-сайтов, информирующих о новых вредоносных программных обеспечениях и оповещает сотрудников о необходимости применения соответствующих мер защиты;

d) обеспечивается точность и информативность предупредительных сообщений. Пользователи осведомляются о проблеме вирусов и действиях при их получении.

По инициативе ответственного за обеспечение ИБ, но на усмотрение руководства Организации возможно использование двух и более защитных программных продуктов от вредоносного кода от различных поставщиков, что может повысить эффективность защиты от вредоносного кода

Антивирусное программное обеспечение должно быть установлено на каждом рабочем компьютере для осуществления автоматических проверок.

Пользователи должны быть уведомлены, а ответственный за обеспечение ИБ быть готов к тому, что возможны случаи обхода антивирусной защиты вирусами или сбои работы антивирусного программного обеспечения.

В таких ситуациях пользователи должны незамедлительно информировать ответственного за обеспечение ИБ о своих подозрениях. Для выявления вируса незамеченного защитным механизмом должны привлекаться соответствующие специалисты. Информация с инфицированного компьютера должна быть проверена и использоваться в изолированной среде, для того чтобы убедиться в отсутствии подозрительной активности.

6. Установка и обновление антивирусных средств

К использованию в Организации допускаются только лицензионные антивирусные средства.

Антивирусное ПО должно обладать следующим функционалом:

a) автоматическое обновление из сети Интернет или централизованного хранилища;

b) автоматическая проверка файлов при обращении к ним;

c) полная проверка всех носителей информации по расписанию;

d) автоматическая проверка критичных зон при запуске рабочей станции и по расписанию;

e) проверка файлов электронной почты;

f) проверка Интернет трафика;

g) проверка файлов в архивах;

h) контроль действий запущенного программного обеспечения;

i) защита от изменения настроек паролем;

j) защита процесса антивирусного ПО;

k) оповещение администратора о подозрительных и зараженных объектах.

Антивирусные программы устанавливаются на все рабочие станции и сервера проекта ИС, системным администратором.

Системный администратор обязан настроить антивирусные средства с соблюдением следующих требований:

a) автоматический запуск антивирусной защиты при запуске программы;

b) запрет на отключение антивирусного ПО и любых проверок;

c) полная антивирусная проверка (сканирование) локальных дисков не реже одного раза в неделю в автоматическом режиме по расписанию;

d) проверка файлов при доступе к ним в автоматическом режиме;

e) обновление антивирусных баз не реже одного раза в три дня;

f) лечение зараженных вирусом файлов, или удаление при невозможности лечения;

g) уведомление о содержащихся вирусах в загружаемых диск файлах и отказ в сохранении;

h) обнаружение и удаление вредоносного программного обеспечения;

i) проверка файлов электронной почты;

j) проверка Интернет трафика;

k) проверка файлов в архивах;

l) контроль действий запущенного программного обеспечения;

m) защита от изменения настроек паролем;

n) защита процесса антивирусного ПО

o) оповещение администратора о подозрительных и зараженных объектах.

7. Порядок проведения антивирусного контроля

Установка (изменение) системного и прикладного обеспечения на рабочих станциях разрешено только в присутствии СОИБ.

Устанавливаемое (изменяемое) на рабочих станциях программное обеспечение должно быть проверено на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

Обязательному антивирусному контролю подлежит любая информация (тестовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация со съемных носителей (магнитные диски, ленты, CD-ROM, и т.п.), получаемых от сторонних лиц и организаций.

Установка (изменение) системного, прикладного и антивирусного обеспечения на серверах проекта ИС осуществляется системным администратором.

Обязательному антивирусному контролю на серверах ИС подлежат все файлы.

Контроль информации на съемных носителях производится непосредственно перед ее использованием.

Особое внимание следует обратить на съемные носители (флэш-накопители, компакт-диски и др.). Работа сотрудников сторонних организаций должна проводиться под непосредственным контролем со стороны СОИБ.

8. Защита от вредоносного программного обеспечения

Сотрудникам проекта на своей рабочей станции запрещено:

– изменять настройки и конфигурацию антивирусных приложений;

– удалять или добавлять какие-либо антивирусные программы;

– работать со съемными дисками без предварительной их проверки, установленной на персональном компьютере антивирусной программой;

– запускать неизвестные приложения, пришедшие по электронной почте, полученные из сети Интернет или из источников, не заслуживающих доверия.

Сотрудник проекта ИС обязан:

– ежедневно в начале работы при загрузке компьютера убедиться в наличии резидентного антивирусного монитора (справа на панели задач должен быть значок с логотипом программы антивирусной защиты и всплывающим над ним наименованием этой программы), и в случае его отсутствия уведомить об этом СОИБ;

– самостоятельно запускать внеплановую антивирусную проверку локальных дисков своего персонального компьютера при получении уведомления от СОИБ о наличии вируса в корпоративной вычислительной сети Организации, а также при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.);

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, незамедлительно сообщить об этом в СОИБ.

Ответственный за обеспечение ИБ обязан:

– контролировать установку и обновление антивирусных программ на рабочих станциях, инструктировать сотрудников по вопросам антивирусного контроля не реже одного раза в неделю;

– контролировать установку и обновление антивирусных программ на серверах ИС не реже одного раза в две недели;

– контролировать настройки модулей антивирусного программного обеспечения не реже одного раза в две недели;

– контролировать актуальность базы антивирусного программного обеспечения не реже одного раза в две недели;

– контролировать состояние антивирусной защиты и эффективность защиты сети от проникновения вредоносного программного обеспечения не реже одного раза в неделю;

– оповещать сотрудников проекта ИС о факте обнаружения заражения вирусом корпоративной информационной сети и выполняемых антивирусных мероприятиях, о проникновении в корпоративную информационную сеть вредоносного программного обеспечения и указания проведенных мер антивирусной защиты.

9. Ответственность

СОИБ несет ответственность за:

a) контроль исполнения требований настоящего документа,
b) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

a) исполнение настоящей Инструкции.

Пользователи ИС:

a) исполнение настоящей Инструкции.