УТВЕРЖДАЮ
Директор ООО «Файнекс»

_____ А.А. Сташевский
20.06.2023

ПОЛОЖЕНИЕ
по организации антивирусной защиты
в ООО «Файнекс»

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение по организации антивирусной защиты в ООО «Файнекс» (далее – Положение) разработано в соответствии с требованиями Политики информационной безопасности ООО «Файнекс» и определяет цели, задачи, организационную структуру антивирусной защиты, а также функциональные обязанности должностных лиц, отвечающих за ее организацию.

1.2. На персональные компьютеры и серверы ООО «Файнекс» (далее – Организация), находящиеся в информационных системах сторонних организаций, распространяются требования по обеспечению антивирусной защиты, которые действуют в данных организациях.

1.3. Для целей настоящего Положения нижеприведенные термины используются в следующих значениях:

ПО – программное обеспечение;

ПК – персональный компьютер;

ЛВС – локальная вычислительная сеть;

антивирусная защита – комплекс организационных и практических мер по защите серверного оборудования, ПК и информационных активов Организации от негативного воздействия вредоносных компьютерных программ и кодов;

компьютерный вирус – вредоносная компьютерная программа или программный код, несанкционированно внедренные в информационную систему Организации, которые могут вызвать нарушение ее работы информационной системы в целом или отдельных компонентов, а также целостность и конфиденциальность информационных активов;

внешние электронные носители информации (далее – ВНИ) – подключаемые к портам ввода-вывода сервера (персонального компьютера) накопители на жестких дисках, CD и DVD дисководы, флэш-накопители, а также иные электронные устройства, имеющие внутреннюю память;

спам – общее обозначение различной информации, которая без запроса поступает пользователю посредством различных средств коммуникации.

1.4. Иные термины, используемые в настоящем Положении, и не указанные в пункте 1.3, имеют значения, определенные нормативными правовыми (техническими нормативными правовыми) актами Республики Беларусь, актами Наблюдательного совета Парка высоких технологий,

Политикой информационной безопасности (кибербезопасности) ООО «Файнекс».

ГЛАВА 2
ЦЕЛИ, ЗАДАЧИ И ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

2.1. Целями антивирусной защиты Организации являются:

предотвращение негативного влияния вредоносных программ на информационную систему Организации или ее компонентов;

обеспечение непрерывности технологических процессов Организации;

обеспечение конфиденциальности и целостности информационных активов Организации.

2.2. Задачи антивирусной защиты:

проверка всех открываемых, сохраняемых и запускаемых файлов на серверах и ПК;

сбор данных о действиях ПО, установленного на серверах и ПК и предоставление этой информации в систему мониторинга событий информационной безопасности;

проверка входящих и исходящих почтовых сообщений на наличие в них вредоносного ПО;

проверка веб-трафика, поступающего на ПК и серверы, а также установка принадлежности интернет-ссылок и адресов к вредоносным или фишинговым веб-ресурсам;

проверка трафика, поступающего на ПК и серверы по протоколам программ для быстрого обмена сообщениями;

периодическая проверка накопителей на жестких магнитных дисках ПК (не реже одного раза в месяц), серверов (по специальному расписанию для каждого сервера) и обязательная проверка используемых в работе мобильных ПК перед началом работы.

2.3. Система антивирусной защиты Организации строится исходя из потенциальных путей проникновения в информационную систему вредоносного ПО, а также связанных с этим рисков потери (снижения) работоспособности информационной системы Организации, нарушения конфиденциальности или целостности информационных активов Организации.

2.4. Основными путями проникновения вредоносных программ и кодов в информационную систему Организации являются:

каналы электронной почты;

страницы сети Интернет с внедренным вредоносным ПО;

внешние электронные носители информации;

написание вредоносной программы непосредственно на рабочем месте работника Организации.

2.5. Для предотвращения негативного воздействия компьютерных вирусов в Организации внедрена система антивирусной защиты, включающая:

средства антивирусной защиты, устанавливаемые на компоненты информационной системы Организации и непосредственно выполняющие функции антивирусной защиты;

режимные и организационные меры обеспечения антивирусной защиты.

2.6. Антивирусные средства устанавливаются:

на ПК работников – в полном объеме;

на почтовом сервере (серверах) – в полном объеме;

на производственных серверах – в соответствии с целесообразностью, обусловленной степенью их уязвимости для вредоносных программ, критичностью реализуемых процессов, наличием иных защитных мер и обстоятельств.

2.7. Средства антивирусной защиты, используемые в Организации, должны иметь сертификаты государственной системы сертификации и реализовывать функции, указанные в Главе 3 настоящего Положения.

2.8. Установленные на ПК и серверах антивирусные средства должны иметь централизованную систему управления. Отключение серверов и ПК от системы централизованного управления антивирусной защитой осуществляется при наличии обоснованной необходимости системным администратором Организации.

2.9. Для повышения эффективности антивирусной защиты в Организации реализуются режимные и ограничительные меры, включающие:

использование режима автоматического обновления антивирусных баз;

установление запрета на отключение пользователями ПК средств антивирусной защиты или изменение их настроек;

выполнение процедур предварительной антивирусной проверки устанавливаемого ПО;

использование средств антивирусной защиты различных производителей и их раздельную установку на рабочих станциях и серверах;

запрет на системном уровне самостоятельной установки работниками на ПК программных средств и средств разработки ПО;

контроль портов подключения ВНИ.

ГЛАВА 3
ОБЩИЕ ТРЕБОВАНИЯ К ФУНКЦИЯМ АНТИВИРУСНОГО ПО

3.1. Обнаруженные антивирусным ПО подозрительные объекты должны помещаться в карантин для последующего анализа системным администратором и принятия решения по дальнейшим действиям с данными объектами.

3.2. Полная антивирусная проверка ПК и серверов должна проводиться автоматически по установленному расписанию, а также инициироваться системным администратором и пользователем ПК.

3.3. Антивирусная проверка почтового сервера должна включать в себя как проверку всех проходящих через почтовую программу потоков, так и хранилища электронных писем. С целью фильтрации спама должна производиться контекстная фильтрация в соответствии со стандартными сигнатурами антивирусного приложения.

Контекстные фильтры добавляются по результатам анализа проходящих к конечным пользователям спам-сообщений.

Подозрительные отфильтрованные сообщения помещаются в карантин, после чего просматриваются системным администратором и, в зависимости от результата, пропускаются адресату или удаляются.

3.4. Антивирусное ПО должно иметь возможность осуществлять централизованный сбор статистики о работе всех установленных антивирусных приложений Организации, отслеживать корректность работы этих приложений и создавать отчеты на основании полученной информации.

3.5. Антивирусные средства должны осуществлять автоматическое сканирование ВНИ, подключаемых к ПК и серверам.

3.6. На ПК работников блокируется возможность изменений настроек или отключения установленного на ПК антивирусного ПО.

3.7. Допускается работа серверов и рабочих станций без средств антивирусной защиты в случае их опытной эксплуатации при условии нахождения в отдельном тестовом сегменте ЛВС.

3.8. Замена версий антивирусного ПО проводится системным администратором в ручном или автоматическом режиме.

3.9. Серверы, на которых установлено ПО сервера антивирусной защиты, устанавливаются в серверных помещениях или, при их отсутствии, в помещениях, имеющих ограниченный доступ.

3.10.Серверы антивирусной защиты должны иметь резервный источник бесперебойного электропитания.

3.11.Инциденты информационной безопасности, связанные с вирусной активностью, дополнительно контролируются системой мониторинга событий системного и прикладного ПО.

ГЛАВА 4
ЗАЩИТА РАБОЧИХ СТАНЦИЙ, НЕ ИМЕЮЩИХ ПОДКЛЮЧЕНИЯ К ЛВС ОРГАНИЗАЦИИ

4.1. На ПК работников, не имеющих подключения к ЛВС Организации, во избежание заражения через сменные МНИ, которые, впоследствии могут стать источниками распространения вредоносных программ на другие ПК и серверы, устанавливается и должно функционировать автономное клиентское антивирусное ПО.

В данном случае ответственность за обновление антивирусных баз и сканирование ПК лежит на работнике Организации, за которым закреплен данный ПК (далее – ответственный работник). Системный администратор обязан проинструктировать ответственного работника о процедуре проведения сканирования на наличие вирусной активности и обновления антивирусных баз.

4.2. Установка обновлений антивирусных баз производится путем скачивания указанных баз с сервера обновления, либо базы переносятся на ПК с помощью USB-накопителей или других ВНИ.

Обновление антивирусного ПО должно производиться ответственным работником не менее одного раза в неделю.

4.3. Сканирование ПК, не имеющих подключения к ЛВС Организации, на наличие вредоносного ПО должно осуществляться не реже чем раз в две недели

ответственным работником в ручном или автоматическом режиме.

ГЛАВА 5
ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ ОРГАНИЗАЦИИ ПО ОБЕСПЕЧЕНИЮ АНТИВИРУСНОЙ ЗАЩИТЫ

5.1. Системный администратор непосредственно отвечает за реализацию мер по обеспечению защиты информационной системы и информационных активов Организации от вредоносных программ и осуществляет:

выявление угроз и оценку рисков, связанных с воздействием на информационную систему и информационные активы Организации вредоносного ПО;

выработку предложений по целям, задачам, структуре и функциям системы антивирусной защиты Организации;

внедрение и эксплуатацию средств антивирусной защиты, поддержание их в работоспособном состоянии;

установку на ПК работников и серверы средств антивирусной защиты до их подключения к ЛВС Организации;

своевременное обновление антивирусных баз;

контроль событий антивирусной защиты, своевременное реагирование на инциденты, связанные с вирусной активностью.

анализ состояния антивирусной защиты и выработку предложений по ее совершенствованию;

реализацию мероприятий по повышению осведомленности работников Организации по вопросам информационной безопасности, в том числе, обеспечения антивирусной защиты;

проведение разбирательств по выявленным фактам нарушений правил антивирусной защиты, заражения ПК вредоносными программами.

5.2. Работники Организации – пользователи ПК, обязаны:

знать и соблюдать правила антивирусной защиты, установленные локальными правовыми актами Организации по работе в информационной системе Организации, использованию ВНИ, ресурсов Интернет;

при подключении ВНИ к ПК осуществлять проверку ВНИ антивирусным средством;

сообщать системному администратору Организации о появлении на экране монитора предупреждающих сообщений о выявлении на ПК вредоносного ПО, выявлении изменений в работе используемого ПО, появлениии графических и звуковых эффектов, искажений данных, частое появление сообщений о системных ошибках и т. п. и иных фактах аномального поведения ПК.