Утверждено:
Приказом № ХХ-П от «__»_____201_ года
Управляющий директор
ОАО «ФИРМА1»

Ф.И.О.

ПОЛИТИКА
антивирусной защиты
ОАО «ФИРМА1»

Город
201_ г.

1. Общие положения.

1.1. Политика антивирусной защиты (далее – Политика) ОАО «ФИРМА1» (далее - Общество) разработана в соответствии с Концепцией безопасности информации Общества, и определяет требования к организации защиты информационно-вычислительной сети (далее – ИВС) от вредоносных программ, с целью предотвращения потери (искажения, перехвата) информации, заражения программного обеспечения, перегрузки и повреждения оборудования ИВС.

1.2. Политика является руководящим документом, единым для всего Общества и обязательным для выполнения всеми работниками Общества.

1.3. Требования данной политики не распространяются напрямую на используемые в Обществе компьютерные системы контроля и управления доступом (СКУД) и теленаблюдения (СТН), но должны быть учтены во внутренних документах Дирекции по режиму и экономической безопасности регламентирующих работу этих систем.

2. Термины и определения.

2.1. **Вредоносная программа** — разновидность компьютерных программ, предназначенных для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы.

К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в информационно-вычислительной сети (далее - ИВС).

2.2. **Вирусный эпизод** – событие, характеризующееся неспособностью антивирусных средств противодействовать активности вредоносной программы по преодолению антивирусной защиты на объекте защиты и распространению на другие объекты защиты информационно-вычислительной сети.

2.3. **Руководители структурных подразделений** - директора, начальники служб, отделов, их заместители, возглавляющие подразделения, напрямую подчиненные Управляющему директору Общества.

3. Объекты антивирусной защиты.

К объектам антивирусной защиты относятся:

- Серверы ИВС;
- Компьютеры (ноутбуки), принадлежащие Обществу, подключенные или периодически подключаемые к ИВС;
- Компьютеры (ноутбуки), принадлежащие Обществу, не подключенные к ИВС Общества, но по специфике их использования предполагается копирование (перенос) информации, содержащейся в них, на ресурсы ИВС или обратно;
- Компьютеры (ноутбуки), принадлежащие третьим лицам и подключаемые к ИВС Общества в рамках заключенных договоров на выполнение работ (оказания услуг);
- Шлюз (шлюзы), соединяющий ИВС Общества с сетью Интернет и другими сетями;
- Корпоративная система электронной почты.

4. Средства антивирусной защиты.

К средствам антивирусной защиты относятся утилиты, программы и программные комплексы, предназначенные для обнаружения и уничтожения вредоносных программ, а также ликвидации последствий, от их воздействий. Все средства антивирусной защиты можно условно разделить на основные и вспомогательные.

4.1. Основные антивирусные средства.

Для постоянной защиты объектов (см. п. 3) должны использоваться программные комплексы в корпоративном исполнении, состоящие из клиентских программ (модулей), устанавливаемых на **каждом из объектов защиты**, программ (модулей) централизованного администрирования, управления и обновления антивирусных баз и самих программ (модулей).

Основные антивирусные средства должны:

- Быть официально приобретены, и использоваться согласно приобретенной лицензии (лицензиям);
- Быть однородными по составу, т.е. должны быть выпущены одним производителем. Допускается использование средств антивирусной защиты других производителей на отдельных объектах защиты, таких, как шлюзы в Интернет (другие сети) и система корпоративной электронной почты;
- Обеспечивать возможность управления (администрирования, конфигурирования, удаленной установки, контроля работы, запуска заданий и т.п.) всеми клиентскими программами с единой консоли (панели) управления администратора;
- Обеспечивать загрузку обновлений антивирусных баз и программного обеспечения через Интернет с серверов обновлений производителя и централизованную установку полученных обновлений с сервера ИВС Общества клиентскими программами, без вмешательства пользователей, с периодичностью не реже 1 раза в час;
- Обеспечивать проверку в режиме реального времени Интернет-трафика, входящих и исходящих сообщений электронной почты, файлов, к которым обращается пользователь или операционная система;
- Обеспечивать недоступность настроек клиентских программ, а также их отключения и деинсталляции для обычных пользователей ИВС;
- Иметь возможность оперативного оповещения пользователей и должностных лиц, отвечающих за антивирусную защиту, обо всех случаях срабатывания антивирусной защиты;
- Иметь в составе средство формирования отчетов.

4.2. **Вспомогательные антивирусные средства.**

Вспомогательные антивирусные средства не предназначены для постоянной антивирусной защиты объектов, и используются периодически специалистами подразделений антивирусной защиты, как дополнительные инструментальные средства для погашения вирусных эпизодов, ликвидации последствий, профилактики заражений и т.п. В качестве вспомогательных средств могут использоваться как платные, так и бесплатные программные антивирусные средства.

Вспомогательные антивирусные средства должны:

- Платные средства должны быть официально приобретены, и использоваться согласно приобретенной лицензии (лицензиям). Бесплатные средства должны использоваться согласно лицензии на их использование;
- Иметь возможность обновления антивирусных баз и самих программ с серверов производителей перед их использованием;
- Быть недоступными для обычных пользователей ИВС.

4.3. **Особенности использования антивирусных средств на некоторых объектах защиты**.

4.3.1. Использование антивирусных средств на серверах ИВС Общества регламентируется Планом антивирусной защиты серверов ИВС, издаваемым Дирекцией по информационным технологиям (далее - ДИТ), согласованным с Дирекцией по режиму и экономической безопасности (далее – ДРиЭБ).

4.3.2. На компьютерах представителей третьих лиц, подключаемых к ИВС Общества, должны быть установлены средства антивирусной защиты, и:

- Быть исправными;
- Обеспечивать загрузку обновлений антивирусных баз и программного обеспечения через Интернет с серверов обновлений производителя;
- Обеспечивать проверку в режиме реального времени Интернет-трафика, входящих и исходящих сообщений электронной почты, файлов, к которым обращается пользователь или операционная система.

Эти требования **должны включаться в договор** на выполнение работ (оказание услуг), заключаемый с третьим лицом. Также в договоре должна быть определена ответственность за невыполнение этих требований.

Перед подключением таких компьютеров к ИВС Общества специалистами ДИТ должна быть проведена их проверка на наличие средств антивирусной защиты и соответствие требованиям, указанным выше.

В случае обнаружения несоответствий антивирусных средств, установленных на компьютере 3 лица хотя бы одному из требований и невозможности их устранения в ходе проведения проверки (например, путем изменения настроек и т.п.), такой компьютер запрещается подключать к ИВС Общества. В этом случае Директор по информационным технологиям должен проинформировать Руководителя структурного подразделения (инициатора), который, в свою очередь, должен принять все меры, направленные на выполнение условий договора третьим лицом.

5. Подразделения антивирусной защиты.

Антивирусная защита в Обществе организуется и проводится во взаимодействии специалистов ДИТ и ДРиЭБ.

5.1. Дирекция по информационным технологиям отвечает за:

- Выбор средств антивирусной защиты, их приобретение, установку на объекты защиты, настройку, сопровождение и обслуживание;
- Анализ вирусной активности в ИВС Общества с целью выявления путей распространения (условий распространения) вредоносных программ;
- Организацию и проведение технических мероприятий по антивирусной защите;
- Погашение вирусных эпизодов и ликвидацию последствий, возникших вследствие воздействий вредоносных программ;
- Разработку документов, устанавливающих правила безопасной работы в ИВС и регламентирующие практические действия пользователей ИВС, специалистов ДИТ в различных ситуациях, связанных с действием вредоносных программ;
- Разъяснительную и профилактическую работу с пользователями ИВС.

5.2. Дирекция по режиму и экономической безопасности отвечает за:

- Проведение расследований вирусных эпизодов с целью выяснения причин и условий их возникновения, путей распространения вредоносных программ, а также лиц виновных в их возникновении;
- Контроль над выполнением требований данной политики и других организационно-распорядительных документов по антивирусной защите.

6. Пользователи средств антивирусной защиты.

Пользователи средств антивирусной защиты – все пользователи ИВС, а также пользователи компьютеров (ноутбуков), не включенных или периодически включаемых в ИВС Общества, а также отдельных компьютеров (ноутбуков), на которых установлены антивирусные средства защиты.

Пользователям средств антивирусной защиты запрещается:

- Предпринимать попытки отключения установленных на компьютерах (ноутбуках) антивирусных программ и их удаления;
- Производить настройки (конфигурирование) антивирусных программ;
- Самостоятельно устанавливать на компьютеры (ноутбуки) любые антивирусные средства;
- Самостоятельно производить устранение последствий от воздействия вредоносных программ;
- Каким либо образом влиять на работу антивирусных программ.

Пользователи средств антивирусной защиты обязаны:

- Немедленно оповещать специалистов ДИТ, ответственных за антивирусную защиту обо всех случаях срабатывания антивирусных средств защиты, установленных на компьютерах (ноутбуке), не подключенных в момент срабатывания к ИВС;
- Немедленно оповещать специалистов ДИТ, ответственных за антивирусную защиту, при

возникновении подозрений на активность вредоносной программы, выражающуюся в нетипичной работе, установленных на компьютере (ноутбуке) программ (приложений), появление графических и звуковых эффектов, искажениях данных, пропадании файлов и директорий, частом появление сообщений о системных ошибках, самостоятельных перезагрузках операционной системы, «подвисаниях» и т.п.

- Проверять антивирусной программой все файлы, полученные из Интернет, посредством электронной почты, а также копируемые на компьютер или ресурс ИВС с любых внешних машинных носителей информации.

7. Ответственность за создание, использование и распространение вредоносных программ.

Согласно статье 273 Уголовного Кодекса Российской Федерации от 13.06.1996 года № 63-ФЗ:

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Приложение: 1. Лист согласования на 1 л. в 1 экз.

Директор по режиму и экономической безопасности ОАО «ФИРМА1» **Ф.И.О.**

Приложение № 1
к Политике антивирусной защиты
ОАО «ФИРМА1»
(на одном листе)

Лист согласования
Политики антивирусной защиты
ОАО «ФИРМА1»

№№ п/п	Должность	Подпись	Фамилия, инициалы	Дата
1	Директор по эксплуатации		Ф.И.О.	
1	Директор по экономике и финансам		Ф.И.О.	
2	Директор по персоналу и общим вопросам		Ф.И.О.	
3	Директор по информационным технологиям		Ф.И.О.	
4	Директор по правовым и корпоративным вопросам		Ф.И.О.	
5	Начальник правового управления		Ф.И.О.	
6	Начальник протокольного отдела		Ф.И.О.	