П Р И К А З

«____»_____**2018 г.** **г. Москва** **№_____**

Об утверждении организации антивирусной защиты ООО «Сатурн»

В целях повышения уровня обеспечения информационной безопасности, информационно-телекоммуникационной инфраструктуры (ИТКИ) Компании,

П Р И К А З Ы В А Ю :

1. Утвердить регламент организации антивирусной защиты ООО «Сатурн» (Приложение №1).
2. Заместителям генерального директора, руководителям функциональных блоков и структурных подразделений организовать изучение Инструкции, указанной в п.1 настоящего приказа, с работниками, и обеспечить выполнение изложенных в ней требований при выполнении своих должностных обязанностей.
3. Контроль исполнения настоящего приказа возложить на …

Генеральный директор
ООО «Сатурн»

Приложение №1
к приказу ООО «Сатурн»
от «__» _____ 2018 г.
№ _____

РЕГЛАМЕНТ
организации антивирусной защиты

1. Аннотация

1.1 Настоящий Регламент разработан в целях установления единых принципов обеспечения антивирусной защиты в ООО «Сатурн» (далее – Компания).

1.2 Настоящий Регламент определяет общие требования к организации антивирусной защиты объектов всех уровней корпоративной локальной вычислительной сети Общества.

1.3 Целевой пользователь документа – работники структурных подразделений Общества.

2. Термины и определения. Принятые сокращения

Термины	Определение
ДИТ	Департамент информационных технологий
ДБ	Департамент по безопасности
ИР	Информационные ресурсы
ИТКИ	Информационно-телекоммуникационная инфраструктура
ИС	Информационная система
СВТ	Средства вычислительной техники
АРМ	Автоматизированное рабочее место
ЛВС	Локальная вычислительная сеть
ПО	Программное обеспечение

3. Основные принципы построения системы антивирусной защиты

3.1. Антивирусной защите подлежат все СВТ ИТКИ.

3.2. Контроль антивирусной защищенности осуществляется непрерывно.

3.3. Управление компонентами антивирусной защиты осуществляется централизованно.

3.4. При выборе антивирусных продуктов учитывается:

– полное соответствие их технических возможностей требованиям настоящего Регламента;

– максимальный охват используемых в ИТКИ платформ и операционных систем одним комплексным решением;

– возможность интеграции в единую систему антивирусной защиты Общества;

– официальная поддержка технологий виртуализации операционных систем и АРМ, используемых СВТ Общества;

– наличие у производителя продукта службы технической поддержки и круглосуточной «горячей» телефонной линии;

– отсутствие недекларированных возможностей продукта, подтвержденное сертификатом ФСТЭК РФ;

– наличие возможности работы в составе системы защиты ИСПДн 1 класса, подтвержденное сертификатом ФСБ России.

4. Задачи антивирусной защиты

4.1. Установка и своевременное обновление (замена) антивирусных пакетов на СВТ ИТКИ.

4.2. Обнаружение компьютерных вирусов и другого вредоносного ПО, оперативное лечение, удаление зараженных объектов и локализация зараженных участков сетевого сегмента с инфицированным АРМ или сервером.

4.3. Своевременное оповещение об обнаруженных или возможных вирусах, их признаках и характеристиках.

4.4. Контроль применения пользователями ИТКИ Общества установленного антивирусного ПО.

4.5. Консультации работников с целью выполнения требований и правил антивирусной защиты.

5. Структура управления

Структура управления системой антивирусной защиты состоит из следующих организационных уровней:

5.1. Руководство Общества – функции общего управления, планирование и финансирование работ по обеспечению антивирусной защиты.

5.2. ДИТ и ДБ – функции управления процедурами организации и контроля функционирования системы антивирусной защиты.

5.3. ИТКИ – реализация функции непосредственной эксплуатации и сопровождения компонентов системы антивирусной защиты.

5.4. Руководители структурных подразделений, пользователи – обеспечение и выполнение процедур эксплуатации средств антивирусной защиты.

6. Общие требования к использованию средств антивирусной защиты

6.1. Допустимо использование только лицензионных средств антивирусной защиты.

6.2. Управление должно осуществляться централизованно на уровне исполнительного аппарата Общества.

6.3. Несанкционированное управление средствами антивирусной защиты (изменение состава компонентов, удаление, отключение защиты, остановка задач и т.п.) недопустимо.

6.4. Программные модули средств антивирусной защиты и пакеты определений вредоносного ПО должны регулярно обновляться в автоматическом режиме:

- проверка наличия обновления программных модулей должна выполняться не реже 1 раза в неделю;
- проверка наличия обновления пакетов определения должна выполняться не реже 2 раз в день;
- при обнаружении обновления, оно должно быть автоматически загружено и установлено на все защищаемые СВТ.

6.5. Антивирусная защита должна осуществляться непрерывно.

6.6. События функционирования средств антивирусной защиты должны протоколироваться.

6.7. Должно быть реализовано оперативное оповещение ответственных лиц о критических и важных событиях антивирусной защиты.

6.8. Средствами антивирусной защиты должна регулярно выполняться полная проверка СВТ на наличие вредоносного ПО, периодичность проверок – не реже 1 раза в неделю.

6.9. При необходимости подключения внешнего устройства хранения данных, пользователь обязан перед началом его использования выполнить полную антивирусную проверку внешнего устройства хранения данных самостоятельно или обратиться в ДИТ.

6.10. При обнаружении вируса или подозрении на его наличие, пользователь обязан немедленно приостановить использование АРМ и безотлагательно обратиться в Департамент информационных технологий, либо в Департамент по безопасности для получения дальнейших инструкций.

6.11. Возможные признаки вирусного заражения:

- соответствующее уведомление средства антивирусной защиты;
- необычное поведение повседневных приложений;
- самопроизвольное появление файлов и папок;
- неустойчивая работа АРМ (перезагрузки, сбои, «зависания»);
- появление непредусмотренных рекламных или информационных сообщений.

6.12. В случае необходимости исключения использования программных средств антивирусной защиты, решение принимается совместно ДИТ и ДБ (за исключением штатного обслуживания).

7. Специальное использование средств антивирусной защиты

7.1. Система антивирусной защиты может использоваться совместно с другими системами и средствами обеспечения информационной безопасности.

7.2. Вирусная активность может быть как следствием, так и причиной НСД к ИТКИ, поэтому анализ информации системы антивирусной защиты является обязательным этапом реагирования на попытки НСД.

7.3. При наличии в ИТКИ централизованной системы мониторинга событий информационной безопасности необходимо обеспечить интеграцию в данную систему отчетной информации системы антивирусной защиты.

8. Требования совместимости

8.1. Применяемые средства антивирусной защиты должны быть совместимы с аппаратными и программными платформами, используемыми в ИТКИ.

8.2. Средства антивирусной защиты не должны нарушать логику работы приложений, защищаемых СВТ.

9. Требования к структуре системы антивирусной защиты

Система антивирусной защиты должна включать в себя компоненты для различных уровней ИТКИ:

9.1. Защита внешних шлюзов.

9.2. Защита серверов.

9.3. Защита АРМ.

10. Функциональные задачи компонентов системы антивирусной защиты

10.1. Задачи защиты внешних шлюзов и серверов общего доступа:

- антивирусная фильтрация трафика и почтовых сообщений;
- антивирусная проверка трафика и почтовых сообщений;
- интеллектуальное перенаправление трафика;
- блокировка распространения вредоносного кода.

10.2. Задачи защиты серверов:

- антивирусная фильтрация трафика в режиме монитора;
- антивирусная проверка трафика в режиме сканера;
- блокировка распространения вредоносного кода;
- лечение зараженных файлов.

10.3. Задачи защиты АРМ:

- антивирусная фильтрация трафика в режиме монитора;
- антивирусная проверка трафика в режиме сканера;
- блокировка распространения вредоносного кода;
- лечение зараженных файлов;
- удаление зараженных файлов;
- контроль использования внешних устройств;
- контроль активности программ;
- персональный сетевой экран;
- функционал обнаружения сетевых атак и вторжений;
- фильтрация почтовых сообщений, анти-спам.

11. Функциональные требования к системе антивирусной защиты

11.1. Сервисные функции:

- контроль работы системы в целом;
- централизованное развертывание всех компонентов системы;
- получение обновлений программного обеспечения и антивирусных баз;
- управление распространением антивирусного программного обеспечения;
- управление обновлением антивирусных баз;
- предоставление отчетной информации.

11.2. Общие функциональные возможности компонентов:

- удаленное управление;
- самозащита от несанкционированного управления;
- ведение журналов;
- оповещение пользователя о важных событиях;

11.3. Требования к центру управления:

- удаленное развертывание средств антивирусной защиты;
- мониторинг состояния антивирусной защиты в режиме реального времени на СВТ ИТКИ;
- централизованное управление лицензионными ключами;
- удаленное управление задачами антивирусной защиты в ручном и автоматическом режиме;
- возможность построения иерархической структуры из нескольких центров управления
- возможность назначения запуска задач по расписанию.

12. Ответственность.

Работники, нарушившие требования настоящего Регламента, могут быть привлечены к дисциплинарной ответственности в соответствии с действующим законодательством РФ.