УТВЕРЖДАЮ

Директор по информационной
безопасности
ООО «Сатурн»

Волков Д.Д.

«___» _____ 2018 г.

РЕГЛАМЕНТ
ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ КОРПОРАТИВНЫХ АНТИВИРУСНЫХ СРЕДСТВ «Kaspersky Endpoint Security» (версия 4.0)

2018 г.

ОГЛАВЛЕНИЕ

1. Общие положения

1.1. Настоящий Регламент устанавливает порядок и правила использования информационной системы «**Kaspersky Endpoint Security**» в ООО «Сатурн» (далее – организация).

1.2. Действие настоящего Регламента распространяется на работников организации, подрядчиков, пользователей и иных лиц при использовании данной информационной системы (далее – ИС).

2. Термины, определения и сокращения

АРМ	Автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи
Администратор ИС	Работник организации ответственный за обеспечение бесперебойного функционирования ИС
Администратор безопасности	Работник организации ответственный за учет съемных накопителей, настройку и реагирование на инциденты, выявленные ИС
Владелец ИС	Лицо, уполномоченное размещать запросы на разработку, доработку, внедрение или приостановку функционирования ИС и сервисов, необходимых для решения бизнес-задач организации
ИБ	Информационная безопасность – комплекс организационных и технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации
ИС	Информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием вычислительной техники
ИТ	Информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку,

	преобразование и передачу информации с использованием средств вычислительной техники
ПК	Персональный компьютер
ПО	Программное обеспечение
Пользователь	Работник Организации, использующий ресурсы информационной системы для выполнения своих должностных обязанностей
Право на доступ	Совокупность правил, регламентирующих порядок и условия доступа пользователя ИС к ее ресурсам
Привилегия на доступ	Исключительное право на доступ к ресурсам ИС
Организация	ООО «Сатурн»
Ответственный за эксплуатацию ИС	Обеспечивает функционирование ИС и отвечает за ее эксплуатацию перед Владельцем ИС. Организует работу Администратора ИС
Реестр	Документ «Реестр разрешенного к использованию ПО». Содержит перечень коммерческого ПО, разрешенного к использованию в Организации
Учетная запись	Информация о пользователе ИС: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.)
Учтенный носитель информации	Съемный накопитель информации, прошедший процедуру учета и маркировку, предназначенный для использования в организации
Backup	Процесс создания копии данных на носителе (жёстком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения

3. Назначение информационной системы

3.1. Информационная система предназначена для обеспечения антивирусной защиты корпоративной ИТ-инфраструктуры организации.

В качестве системы антивирусной защиты корпоративной ИТ-инфраструктуры применяется программный комплекс «Kaspersky Security Center».

3.2. Решаемые задачи

- Защита рабочих станций;
- Защита файловых серверов;
- Системное администрирование;
- Шифрование конфиденциальной информации;
- Безопасность мобильных устройств;
- Контроль программ, устройств и веб-ресурсов;
- Централизованное управление.

3.3. Характеристики ИС

Лицензированные технологии	Стандартный
Рабочие станции	✓
Защита от вредоносного ПО	✓
Сетевой экран	✓
Контроль программ	✓
Контроль устройств и Веб-Контроль	✓
Шифрование данных	✓
Файловые серверы	✓
Мобильные устройства	✓

4. Состав ИС

4.1. Аппаратная часть включает

- Виртуальная машина: ОС win_ser_64, число ядер 4 - 8, память 8Гб, HDD под систему 300Гб, HDD под хранилище 2000Гб.

4.2. Программная часть включает

- Kaspersky Security Center 10

4.3. Инфраструктура ИС

Наименование (Hostname)	IP management
vm-kav	10.10.**.**

5. Потребители информационной системы

5.1. Владелец ИС, Ответственный за эксплуатацию ИС и Администратор ИС назначаются Приказом Генерального директора ООО «Сатурн»

- **Владелец ИС** – лицо, выполняющее роль заказчика конкретной ИС со стороны руководства ООО «Сатурн». Владелец ИС отвечает за эксплуатацию ИС перед руководством ООО «Сатурн», утверждает регламент использования ИС, уполномочен размещать запросы на ввод в эксплуатацию ИС, разработку, доработку, внедрение подсистем и сервисов, необходимых для решения задач бизнес-процессов компании.
- **Ответственный за эксплуатацию ИС** – обеспечивает функционирование ИС и отвечает за ее эксплуатацию перед Владельцем ИС. Организует работу Администратора ИС, взаимодействие с Департаментом ИТ ООО «Сатурн», пользователями ИС и другими заинтересованными сторонами.
- **Администратор ИС** – непосредственно обеспечивает настройку и администрирование ИС на прикладном и/или системном уровне. Взаимодействует с администраторами Департамента по ИТ ООО «Сатурн» осуществляющими администрирование ИС на системном уровне.

5.2. Потребителями информационной системы являются:

- Сотрудники службы ИБ

6. Используемые в ИС учетные записи

6.1. Учетная запись пользователя ОС

- Доменная учетная запись «*****»

6.2. Учетная запись пользователя ПО консоли «Kaspersky Endpoint Security»

- Доменная учетная запись «*****»

6.3. Учетная запись сервисная ПО «Kaspersky Endpoint Security»

- Доменная учетная запись «*****»

7. Порядок предоставления прав доступа

7.1. Для получения или изменения прав доступа необходимо получить согласование от Владельца ИС и службы ИБ.

8. Управление доступом

8.1. Доступ к информационной системе осуществляется:

- Путем авторизации по логину и паролю

8.2. Требование к парольной защите:

- Длина пароля не менее 8 символов английского алфавита включая символы и цифры

8.3. Периодичность смены пароля:

- Не реже 1 раза в квартал или по указанию службы ИБ

8.4. Смена пароля осуществляется Администратором ИС. Текущий пароль передаётся Администратором ИС в службу ИБ.

9. Доступ в помещения и к техническим средствам ИС

9.1. Доступ в помещения, где установлены технические средства ИС ограничен и осуществляется в соответствии с Регламентом доступа в серверные и кроссовые помещения.

9.2. Шкафы с установленными техническими средствами должны быть закрыты на ключ. Ключи хранятся у Ответственного за эксплуатацию ИС.

9.3. Технические средства ИС должны быть опечатаны специальным защитным знаком. Вскрытие опечатанных технических средств возможно только с разрешения Ответственного за эксплуатацию ИС и по согласованию со службой ИБ.

9.4. Перечень опечатанных технических средств с указанием номеров защитных знаков хранятся у службы ИБ.

10. Порядок внесения изменений в ИС

10.1. Любые изменения в состав, архитектуру или порядок использования ИС осуществляются только по согласованию с Владельцем ИС и службой ИБ.

10.2. Доработки должны производиться только по утвержденному Владельцем ИС и согласованному с службой ИБ техническому заданию, которое должно включать:

- Цель доработки/обновления/внесения изменений;
- Решаемые задачи;
- Сроки выполнения работ;
- Состав исполнителей (рабочей группы);
- Порядок приемки и критерии оценки успешности выполняемых работ.

10.3. Все изменения должны быть зафиксированы и задокументированы.

11. Управление лицензиями ПО

11.1. Лицензии на программное обеспечение, входящее в состав ИС:

- Находятся в ведении службы ИБ

12. Мониторинг состояния ИС и отчетность

12.1. Мониторинг состояния ИС осуществляется с использованием ИС «PRTG». Мониторинг осуществляется как минимум в части следующих параметров ИС:

- Доступность (PING);
- Загрузка процессора (%);
- Загрузка жесткого диска (%);
- Загрузка интерфейса менеджмента (кбит/с);
- Загрузка интерфейса данных (кбит/с);
- Доступная оперативная память (%).

12.2. Отчетность по результатам работы ИС должна формироваться еженедельно по средам в формате PDF-файла и должна включать:

- Наименование отчета;
- Период, за который сформирован отчет;
- Отчет об обнаруженных и предотвращенных угрозах.

13. Организация резервного копирования (Backup)

13.1. Резервному копированию подвергаются следующие компоненты ИС

- Полный образ системы с установленным ПО

13.2. Резервное копирование выполняется следующими техническими средствами

- ПО «*****»

13.3. Периодичность выполнения резервного копирования

- Не реже одного раза в неделю

13.4. Резервное копирование производится администратором ИС

13.5. Резервное копирование осуществляется

- Указать куда

14. Порядок внесения изменений и дополнений в Регламент

14.1. Изменения и дополнения в настоящий Регламент вносятся ответственными за эксплуатацию ИС и утверждаются Владельцем ИС.

14.2. Все изменения и дополнения настоящего Регламента вступают в силу с момента их утверждения.

Ведущий специалист по ИБ Смирнов В.В.