П Р И К А З

«____»_____2018 г. г. Москва №_____

Об утверждении инструкции работы администраторов и пользователей в корпоративной сети ООО «Сатурн»

В целях обеспечения раннего предупреждения угроз и усиления контроля состояния информационной безопасности в ООО «Сатурн»:

1. Утвердить инструкцию работы администраторов и пользователей в корпоративной сети 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 …

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

ИНСТРУКЦИЯ
работы администраторов и пользователей в корпоративной сети ООО «Сатурн»

1. Аннотация

1.1. Настоящая Инструкция разработана в целях регламентации работы на автоматизированных рабочих местах (далее – АРМ) в локальной вычислительной сети ООО «Сатурн» (далее - Компания) с точки зрения повышения уровня информационной безопасности в Компании.

1.2. Настоящая Инструкция призвана гарантировать надлежащее использование АРМ и информационно-телекоммуникационной инфраструктуры работниками.

1.3. Целевой пользователь документа – работники структурных подразделений Общества.

1.4. Термины и определения. Принятые сокращения

Термин	Определение
Компания	ООО «Сатурн»
ДБ	Департамент по безопасности
ИР	Информационные ресурсы
ИС	Информационная система (например, персональный компьютер, файловое хранилище, электронная почта, ресурсы сети Интернет и др.)
ДИТ	Департамент информационных технологий
ИТКИ	Информационно-телекоммуникационная инфраструктура
СВТ	Средства вычислительной техники
АРМ	Автоматизированное рабочее место
ЛВС	Локальная вычислительная сеть
ПО	Программное обеспечение
НСД	Несанкционированный доступ

2. Общие положения

2.1. В целях обеспечения режима коммерческой тайны (конфиденциальности), доступности и целостности информационных ресурсов доступ к корпоративным ИС должен предоставляться только авторизованным пользователям и только в том объеме, в каком он требуется для выполнения ими должностных обязанностей. Компания должно управлять процессом предоставления доступа в ИС и контролировать использование предоставленного доступа.

2.2. ЛВС является основной составляющей ИТКИ, совокупностью аппаратных и программных средств, средой передачи информационных и управляющих сигналов.

2.3. ЛВС предназначена для:

организации доступа пользователей к закрепленным за ними АРМ и использования их для выполнения своих служебных функций;

организации и разделения доступа к ИР;

подготовки, передачи, хранения и использования информации;

организации группового доступа к принтерам и другим периферийным устройствам;

организации работы корпоративной электронной почты;

централизованного доступа к сети Интернет;

обеспечения работы информационных систем.

2.4. ЛВС включает в себя:

сервера и сетевое оборудование, обеспечивающие работу ЛВС, ролевой доступ к ИР;

учетные записи администраторов и пользователей;

почтовые сервера;

сетевые ресурсы общего, группового и индивидуального доступа, предназначенные для хранения файлов;

точки доступа в Интернет;

прокси-сервера, обеспечивающие контролируемый доступ пользователей в Интернет;

другие аппаратные и программные элементы, обеспечивающие соединения и работоспособность ЛВС, и иное периферийное оборудование;

АРМ администраторов и пользователей.

2.5. Ответственные за бесперебойное функционирование ЛВС и предоставление пользователям доступа (далее - Администраторы) определяются в соответствии с сервисными договорами или должностными инструкциями сотрудников ДИТ.

2.6. Доступ в ЛВС и предоставление адреса корпоративной электронной почты производится работниками ДИТ или представителями компаний подрядчиков (на основании действующих договоров) в порядке, установленном действующими в Компании регламентирующими документами.

2.7. Доступ к ресурсам Интернет предоставляется пользователям для выполнения прямых должностных обязанностей, делового общения и сбора информации по ключевым задачам деятельности в соответствии с должностной инструкцией.

2.8. В целях обеспечения нормального функционирования ИТКИ пользователи обязаны соблюдать настоящую Инструкцию, другие инструкции по пользованию ресурсами ИТКИ, утвержденные в установленном порядке, а также следовать рекомендациям администраторов ДИТ и работников ДБ.

3. Функции роли администратора

3.1. Администратор обладает всей полнотой доступа к ресурсам ИТКИ, организует и контролирует их работу, объектов информатизации и других пользователей.

3.2. Администратор в своей работе руководствуется и исполняет функции, предусмотренные настоящей инструкцией и иными инструкциями и организационной-распорядительными документами Общества.

3.3. Основные обязанности Администратора:

обеспечивает доступ пользователей к ЛВС, корпоративной электронной почте, сетевым ресурсам и Интернету;

обеспечивает постоянную работоспособность ИТКИ;

контролирует доступность для пользователей сети Интернет;

обеспечивает функционирование и поддерживает работоспособность средств и систем защиты информации в пределах возложенных функциональных обязанностей;

принимает меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью предотвращения последствий;

в случае отказа элементов ИТКИ, принимает срочные меры по их восстановлению;

сообщает руководству ДИТ и ДБ о ставших ему известными признаках НСД;

ведет предусмотренную документацию на ИТКИ.

3.4. Основные права Администратора:

требовать от пользователей выполнения правил пользования ресурсами ИТКИ, утвержденных в установленном порядке;

прекращать доступ пользователей к ИР, в случае неисполнения ими требований правил пользования ресурсами ИТКИ, утвержденных в установленном порядке.

3.5. Требования Администратора в части пользования ИР и СВТ обязательны для всех пользователей.

3.6. В случае несогласия пользователей с действиями Администратора, они могут быть обжалованы руководству ДИТ и ДБ.

4. Права и обязанности пользователей

4.1. Пользователь ИТКИ имеет право:

пользоваться в служебных целях закрепленным АРМ, корпоративной электронной почтой, Интернетом, предоставленными сетевыми ресурсами и программным обеспечением;

обращаться к специалистам ДИТ или сотрудникам подрядных организаций, предоставляющих услуги технической поддержки в соответствии с сервисными договорами за консультацией по вопросам функционирования АРМ, ЛВС или работы программных продуктов;

изменять свои пароли, в соответствии с политикой парольной защиты информационных ресурсов;

требовать у работников ДИТ обеспечения бесперебойной работы АРМ, ЛВС;

4.2. Пользователь ИТКИ обязан:

4.2.1. Обладать необходимыми навыками работы с используемым аппаратным и программным обеспечением. Выполнять на АРМ только те процедуры, которые определены для него должностной инструкцией;

4.2.2. Руководствоваться требованиями, предусмотренными настоящей инструкцией и иными регламентирующими документами, утвержденными в установленном порядке:

– Инструкция по резервному копированию и восстановлению информационных ресурсов;

– Регламент реагирования на попытки доступа к информационным ресурсам со стороны пользователей и администраторов сети;

– Регламент организации антивирусной защиты;

– Правила парольной защиты информационных ресурсов.

4.2.3. При работе на АРМ использовать только персональные идентификационные данные.

4.2.4. Вести всю служебную переписку только с использованием персонального адреса корпоративной электронной почты.

4.2.5. Контролировать размер файлов, отправляемых по электронной почте (рекомендуемый объём электронного сообщения – не более 5 мегабайт).

4.2.6. Следить за состоянием и исправностью предоставленных технических средств.

4.2.7. Информировать специалистов ДИТ и ДБ о признаках обнаружения вирусов, попыток несанкционированного доступа.

4.2.8. При выполнении работ, предполагающих интенсивную загрузку ЛВС (передача, получение значительного по объему количества данных, высокое количество сетевых соединений), заранее оповещать специалистов ДИТ.

4.3. Пользователю ресурсов ИТКИ **запрещается**:

– устанавливать, модифицировать или хранить программное обеспечение без согласования с ДИТ;

– самостоятельно разбирать, вносить изменение аппаратной конфигурации на закрепленном АРМ;

– устанавливать удаленный доступ к закрепленному АРМ без разрешения руководства ДБ и ДИТ;

– использовать доступ в Интернет в личных целях, противоречащих законодательству РФ, положениям организационно-распорядительных документов Компании, должностной инструкции;

– изменять параметры и роль предоставленной учетной записи;

– хранить личную информацию на файловых ресурсах ИТКИ;

– запрещается хранение или передача в открытом виде информации, ограничения на которую распространяются в федеральном законодательстве

РФ и организационно-распорядительных документах Общества (государственная тайна, персональные данные, коммерческая тайна и пр.).

5. Рекомендации и ограничения общего характера

5.1. В части хранения паролей:

– Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

– Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

5.2. В части использования электронной почты:

– Отключите поддержку расширенного текстового формата и HTML-формата электронных писем;

– Проверяйте вложения в сообщениях электронной почты перед открытием на наличие исполняемых файлов, при наличии их - избегайте их запуска;

– Избегайте перехода по гиперссылкам, содержащимся в электронных письмах.

5.3. В части просмотра интернет ресурсов:

– Не рекомендуется переход по баннерам и рекламным объявлениям на веб-сайтах;

– Не посещайте недоверенные и нелегальные веб-сайты;

– Не переходите по подозрительным ссылкам, таким как ссылки на .EXE-файлы;

– Не загружайте и не устанавливайте нелицензионное программное обеспечение, так как это программное обеспечение может содержать скрытые вредоносные программы;

– Не осуществляйте работу при отключенных средствах защиты (антивирус и других);

– Не передавайте защищаемую информацию без использования средств защиты;

– Не снижайте уже установленного уровня защищенности информации (например: при получении письма в защищенном виде по электронной почте не пересылайте его в открытом виде).

6. Обязанности руководителей структурных подразделений ООО «Сатурн»

6.1. Ознакомить под роспись подчиненный персонал с содержанием настоящей Инструкции и обеспечивать ее соблюдение.

6.2. В течение двух рабочих дней уведомить ДИТ и ДБ об увольнении сотрудников, принятии на работу, отпуске и изменении в занимаемой должности.

6.3. Выносить предложения ДБ и ДИТ по совершенствованию положений настоящей Инструкции, вносить дополнения и корректировки.

7. **Ответственность**

7.1. Пользователь несет ответственность за сохранность и надлежащую эксплуатацию выделенного АРМ и установленного на нем программного обеспечения, а также несет ответственность за информационный обмен между его персональным компьютером, другими компьютерами Общества и компьютерами за пределами Общества.

7.2. Работники несут ответственность за все действия, совершенные от их имени, с использованием их идентификационных данных.