П Р И К А З

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

Об утверждении порядка контроля журналов аудита основных информационных ресурсов и реагирования на попытки доступа к информационным ресурсам со стороны пользователей и администраторов сети, на инциденты, касающиеся сбоев в работе систем, вирусного заражения и других событий информационной безопасности

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

1. Утвердить порядок реагирования на попытки доступа к информационным ресурсам со стороны пользователей и администраторов сети, на инциденты, касающиеся сбоев в работе систем, вирусного заражения и других событий информационной безопасности в ООО «Сатурн» (Приложение № 1).
2. Утвердить порядок контроля журналов аудита основных информационных ресурсов в ООО «Сатурн» (Приложение № 2).
3. Руководителям 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
4. Ответственного за ведение и контроль журналов аудита назначить ….
5. Контроль исполнения настоящего приказа возложить ….

Генеральный директор
ООО «Сатурн»

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

ПОРЯДОК
реагирования на попытки доступа к информационным ресурсам со стороны пользователей и администраторов сети, на инциденты, касающиеся сбоев в работе систем, вирусного заражения и других событий информационной безопасности

1. Аннотация

1.1. Настоящий регламент разработан на основе требований к информационной безопасности и определяет комплекс организационно-технических мер по защите информационно-телекоммуникационной инфраструктуры от несанкционированного доступа к циркулирующей в ней информации, а также незаконного вмешательства в процесс ее функционирования.

1.2. Целевой пользователь документа – работники структурных подразделений ООО «Сатурн».

2. Термины и определения. Принятые сокращения

Термин	Определение
ДИТ	Департамент информационных технологий
ДБ	Департамент по безопасности
ИР	Информационные ресурсы
ИС	Информационная система
ИТКИ	Информационно-телекоммуникационная инфраструктура
СВТ	Средства вычислительной техники
АРМ	Автоматизированное рабочее место
ЛВС	Локальная вычислительная сеть
ПО	Программное обеспечение
НСД	Несанкционированный доступ
Нарушитель	Физическое лицо, которое предприняло попытку выполнения запрещенных в ИТКИ действий
СКУД	Система контроля и управления доступом

3. Общие положения

3.1. Основной целью разработки настоящего Регламента является защита ИТКИ от возможного нанесения вреда посредством случайного или преднамеренного несанкционированного вмешательства в процесс ее функционирования, предупреждение и пресечение несанкционированного доступа к конфиденциальной информации.

3.2. Алгоритм реагирования на НСД основан на элементах системы обеспечения информационной безопасности:

− физическая защита. Все помещения, где расположены аппаратные средства ИТКИ, находятся под охраной и защищены СКУД;

− нормативное регулирование. В Компании утверждены организационно-распорядительные документы (Далее – ОРД) по организации пользования средствами ИТКИ. Все работники ознакомлены с утвержденными правилами и предупреждены об ответственности за их нарушение;

− программные средства защиты, которые включают в себя комплекс мер и мероприятий:

- разграничение доступа;
- средства идентификации пользователей;
- средства сетевой защиты;
- защита исполняемых файлов от изменения;
- замкнутая среда разрешенных для запуска программ для каждого пользователя системы;
- периодический контроль целостности системы;
- система регистрации событий;
- оперативное оповещение администратора об активности рабочих станций сети и пользователей, а также обо всех происходящих на рабочих станциях попытках НСД;
- средства парольной защиты;
- антивирусная защита.

3.3. При определении алгоритма действий в случае выявления НСД к ИТКИ учитывается:

− доступ к ИР должны иметь только зарегистрированные в установленным порядке пользователи;

− доступ зарегистрированных пользователей к аппаратным, программным и информационным ресурсам должен быть разграничен;

− действия пользователей при работе с защищаемыми ресурсами должны регистрироваться в системных журналах;

− массивы данных ИТКИ должны иметь защиту от несанкционированной утечки, модификации, фальсификации, уничтожения и подтверждение аутентичности.

4. НСД и виды нарушителей

4.1. Алгоритм реагирования на НСД предназначен для недопущения и пресечения причинения вреда интересам Общества:

− возникновение незарегистрированного или незащищенного доступа к ИТКИ;

− раскрытие конфиденциальной информации;

− остановка или нарушения в работе ИТКИ.

4.2. НСД подразделяются на следующие группы:

− Уровень 1 – критическое событие. Имеются явные признаки совершения НСД с использованием серьезной уязвимости в системе безопасности системы;

− Уровень 2 – событие, требующее немедленного вмешательства. Вероятность НСД, вызванного уязвимостью, очень высока;

− Уровень 3 – проблема с элементами ИТКИ, требующая проверки и устранения в сжатые сроки.

4.3. Система защиты ИТКИ строится из следующих предположений о возможных типах Нарушителей:

− Неопытный (невнимательный) пользователь - пользователь, который может предпринимать попытки выполнения запрещенных операций, действуя по ошибке, некомпетентности или халатности и использующий при этом только штатные аппаратные и программные средства;

− Любитель - пользователь, совершающий при работе в ИТКИ запрещенные действия без прямого умысла на получение доступа к закрытым для него ресурсам или причинения вреда ИТКИ с использованием как штатных, так и дополнительных средств;

− Злоумышленник - лицо, действующее умышленно, из корыстной или иной заинтересованности, с целью получения доступа к закрытым для него ресурсам или причинения вреда ИТКИ. Злоумышленники по уровню доверенности подразделяются:

- Внутренний – пользователь, официально получивший доступ в ИТКИ, имеющий разрешения на пользование АРМ, включенного в ЛВС;
- Внешний - лицо, не имеющее официальных прав на доступ в ИТКИ.

4.4. Действия нарушителей могут быть направлены на:

− создание удаленных подключений, не санкционированных в установленном порядке;

− преодоление запретов и ограничений, предусмотренных для предоставленных учетных записей пользователей;

− получение доступа к закрытым сетевым ресурсам, аппаратным и программным средствам;

− изменение ПО, изменение конфигурации аппаратных средств, внедрение программных закладок и т.п.

5. Журналы аудита событий ИТКИ

5.1. Основным средством объективного контроля и выявления НСД является ведение журналов аудита.

5.2. Журналы аудита обеспечивают обнаружение и регистрацию событий, которые могут повлечь за собой нарушение политик безопасности и возможности НСД;

5.3. Формирование, ведение и содержание журналов аудита должно обеспечивать:

− оперативное ознакомление администратора с содержимым журналов;

− систематизацию журналов и содержащейся в них информации по датам и времени;

− оперативное оповещение (выделение информации) о нарушениях безопасности;

− предоставление достаточной для идентификации событий информации, в том числе:

- дата и время события;
- идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
- действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

5.4. Перечень журналов аудита определяется исходя из структуры ИТКИ, количества серверов, самостоятельных элементов.

5.5. Резервное копирование и восстановление журналов аудита производится в соответствии с Инструкцией по резервному копированию и восстановлению информационных ресурсов Общества.

6. Порядок действий при обнаружении признаков НСД

6.1. Признаки НСД могут быть выявлены в процессе анализа журналов событий, а также при использовании СВТ всеми пользователями ИТКИ:

− антивирусное программное обеспечение активно детектирует вирусы, сетевые черви, трояны и т.п.;

− в операционной системе появились неизвестные учетные записи;

− отказ или медленная работа сети;

− отказ в доставке и отправке почты;

− отказ периферийных сетевых устройств;

− удаление или изменение свойств и содержания файлов;

− возникают ошибки входа в систему;

− происходят самопроизвольные перезагрузки компьютера;

− возникли ошибки при загрузке компьютера.

6.2. Признаки НСД могут быть выявлены в процессе проведения плановых проверок АРМ пользователей и тестирования ИТКИ.

6.3. В случае выявления признаков НСД пользователи обязаны:

− максимально быстро выполнить корректное завершение работы компьютера (Пуск → Завершение работы);

− сообщить о произошедшем в ДИТ и ДБ;

− действовать в соответствии с рекомендациями сотрудников ДИТ и ДБ.

6.4. При получении информации о признаках НСД Администратор безопасности обязан:

− принять срочные меры по проверке информации, выявлению причин неполадок и оценке их опасности;

− в случае наличия достаточных признаков, подтверждающих совершение НСД, принять срочные меры по прекращению НСД, отключению аппаратного или программного средства ИТКИ, к которому или от имени, которого совершено НСД;

− доложить о происшествии руководителям ДИТ и ДБ.

6.5. По результатам анализа обстоятельств происшествия, информации о типе нарушителя, выполняются следующие мероприятия:

− ДИТ совместно с ДБ принимаются меры к фиксации признаков НСД и установлению нарушителя;

− информация о происшествии направляется Директору по комплексной безопасности для принятия решения о назначении служебной проверки;

− по результатам служебной проверки принимается решение о привлечении виновных к дисциплинарной и материальной ответственности. Вырабатываются меры по недопущению подобных происшествий в будущем.

− Если попытка НСД совершена из внешней среды, дополнительно направляется соответствующая информация в ДБ.

7. Контроль и ответственность

7.1. Контроль соблюдения требований настоящего Регламента осуществляется ___ совместно с ___ путём проведения плановых и внеплановых проверок.

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

Приложение №2
к приказу ООО «Сатурн»
от «__» _____ 2018 г.
№ _____

ПОРЯДОК
контроля журналов аудита основных информационных ресурсов ООО «Сатурн»

1. Введение

Настоящий Порядок служит для обеспечения контроля доступа к информационным активам (операционным системам, приложениям, информационным системам и т.п.), а также для обеспечения порядка аудита информационных активов ООО «Сатурн» (далее - Компания), с учетом внутренних организационно-распорядительных документов (Далее – ОРД) Общества и требований информационной безопасности.

2. Порядок контроля доступа

2.1. Контроль доступа к операционным системам

Для предотвращения неавторизованного доступа к компьютерам на уровне операционной системы (далее - ОС) необходимо использовать средства обеспечения безопасности, которые должны предусматривать:

- идентификацию и верификацию компьютера пользователя, терминала и местоположения каждого авторизованного пользователя;
- регистрацию успешных и неудавшихся доступов к системе;
- аутентификацию соответствующего уровня.

Для обеспечения контроля неавторизованного доступа в ОС необходимо ведение журналов аудита ОС (по умолчанию – журнал ОС «Безопасность»).

2.2. Контроль доступа к приложениям

Для предотвращения неавторизованного доступа к данным информационной системы (далее - ИС) необходимо применять меры обеспечения безопасности для ограничения доступа к прикладным системам (приложениям).

Требования контроля доступа к приложениям должны включать:

- обеспечение доступа пользователям приложений к информации и функциям этих приложений;
- для обеспечения контроля неавторизованного доступа в ИС необходимо ведение журналов аудита ИС.

3. Порядок ведения аудита

Для обнаружения неавторизованных действий Департамент информационных технологий и Департамент по безопасности проводят мониторинг системы.

Требования к мониторингу доступа:

- ведение журналов аудита на всех информационных активах Общества (таких как операционные системы, базы данных, информационные

системы и т.п.), в пределах функциональных возможностей информационных активов. В информационных активах должны отражаться события, связанные с безопасностью, а также обеспечиваться хранение указанных журналов;

- записи аудита должны включать (при функциональной возможности ИС):

1) идентификатор пользователей;
2) даты и время входа и выхода;
3) идентификатор терминала или его местоположение;
4) записи успешных и отклоненных попыток доступа к ИС;
5) записи успешных и отклоненных попыток доступа к данным и другим информационным активам;

- журналы аудита должны регулярно проходить анализ при помощи специализированных программно-аппаратных средств.