УТВЕРЖДАЮ:
«__» _____ 20__ г.

СТО № ИБ.002

Регламент управления уязвимостями информационной безопасности ООО «Сатурн»

Версия 1.0

Москва
2018

Сведения о нормативном документе

Информация о документе	
Функциональный руководитель	
Разработчик документа	
Введен в действие	Приказом № _____ от ___.___._____
Срок действия	не ограничен

История изменений			
Дата	**Версия**	**Автор изменений**	**Причина внесения изменений**

Содержание

1. Цель и область действия

1.1 Цель Регламента

Целью разработки Регламента управления уязвимостями информационной безопасности ООО «Сатурн» (далее – Регламент) является повышение уровня информационной безопасности ООО «Сатурн» посредством повышения защищенности информационной инфраструктуры и информационных систем ООО «Сатурн»

1.2 Область действия

1.2.1 **Потребность в реализации процесса:**

Процесс управления уязвимостями является одной из составных частей процесса управления рисками информационной безопасности ООО «Сатурн».

1.2.2 **Результаты выполнения процесса:**

Перечни актуальных и устраненных уязвимостей информационной безопасности для активов ООО «Сатурн».

1.2.3 Настоящий Регламент:

1.2.3.1 Определяет системный подход к процессу управления уязвимостями информационной безопасности ООО «Сатурн».

1.2.3.2 Описывает этапы процесса управления уязвимостей и его участников, а также их действия на каждом этапе.

1.2.3.3 Распространяется на Активы ООО «Сатурн», находящиеся в зоне ответственности Комплекса по стратегии.

1.3 Ответственный за актуализацию

Ответственным за актуализацию настоящего Регламента является Директор по эксплуатации систем информационной безопасности ООО «Сатурн».

2. Нормативные ссылки

2.1 ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения.

2.2 ГОСТ Р 56546-2015. Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

3. Термины и сокращения

3.1 В настоящем Регламенте использованы следующие сокращения:

3.1.1 ИБ – Информационная безопасность

3.1.2 ДИБ – Дирекция по информационной безопасности ООО «Сатурн»

3.1.3 КпС – Комплекс по стратегии ООО «Сатурн»

3.1.4 СКЗСС – Система контроля защищенности и соответствия стандартам на базе программного обеспечения MaxPatrol, (также для употребления в рамках ООО «Сатурн» может применяться название «Система контроля и анализа защищенности»).

3.2 В настоящем Регламенте использованы следующие термины:

3.2.1 Активы – программное обеспечение и программно-технические средства (включая их окружение) как отдельно, так и в составе автоматизированных и информационных систем, в том числе находящиеся в эксплуатации и планируемые к внедрению/разработке, находящиеся в зоне ответственности Комплекса по стратегии.

3.2.2 Процесс – процесс управления уязвимостями информационной безопасности.

3.2.3 Угроза безопасности информации (угроза информационной безопасности) - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения информационной безопасности.

3.2.4 Уязвимость - недостаток (слабость) Актива, который (которая) может быть использована для реализации угроз безопасности информации (информационной безопасности).

3.2.5 Уязвимость кода - уязвимость, появившаяся в процессе разработки программного обеспечения.

3.2.6 Уязвимость конфигурации - уязвимость, появившаяся в процессе задания конфигурации (применения параметров настройки) Актива.

3.2.7 Уязвимость архитектуры - уязвимость, появившаяся в процессе проектирования Актива.

3.2.8 Уязвимость организационная - уязвимость, появившаяся в связи с отсутствием (или недостатками) организационных мер защиты информации в информационной системе и (или) несоблюдением требований локальных нормативных актов Корпорации по информационной безопасности и (или) несвоевременном выполнении соответствующих действий должностным лицом (работником) или подразделением, ответственными за информационную безопасность.

3.2.9 Уязвимость многофакторная - уязвимость, появившаяся в результате наличия нескольких недостатков различных типов.

3.2.10 Участники Процесса – Сотрудники ДИБ, КпС.

4. Общие положения

4.1 Классификация и типы уязвимостей в отношении которых действует Регламент соответствуют ГОСТ Р 56546-2015. Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

4.2 Процесс управления уязвимостями информационной безопасности включает в себя следующие основные процедуры:

4.2.1 Идентификация уязвимостей.

4.2.2 Анализ уязвимостей.

4.2.3 Устранение уязвимостей.

4.3 Все Активы, подключенные к информационной инфраструктуре ООО «Сатурн», должны быть подключены к СКЗСС.

4.4 Для повышения оперативности и эффективности Процесса, все проводимые в рамках исполнения положения Регламента коммуникации и операций, должны документироваться в электронном виде.

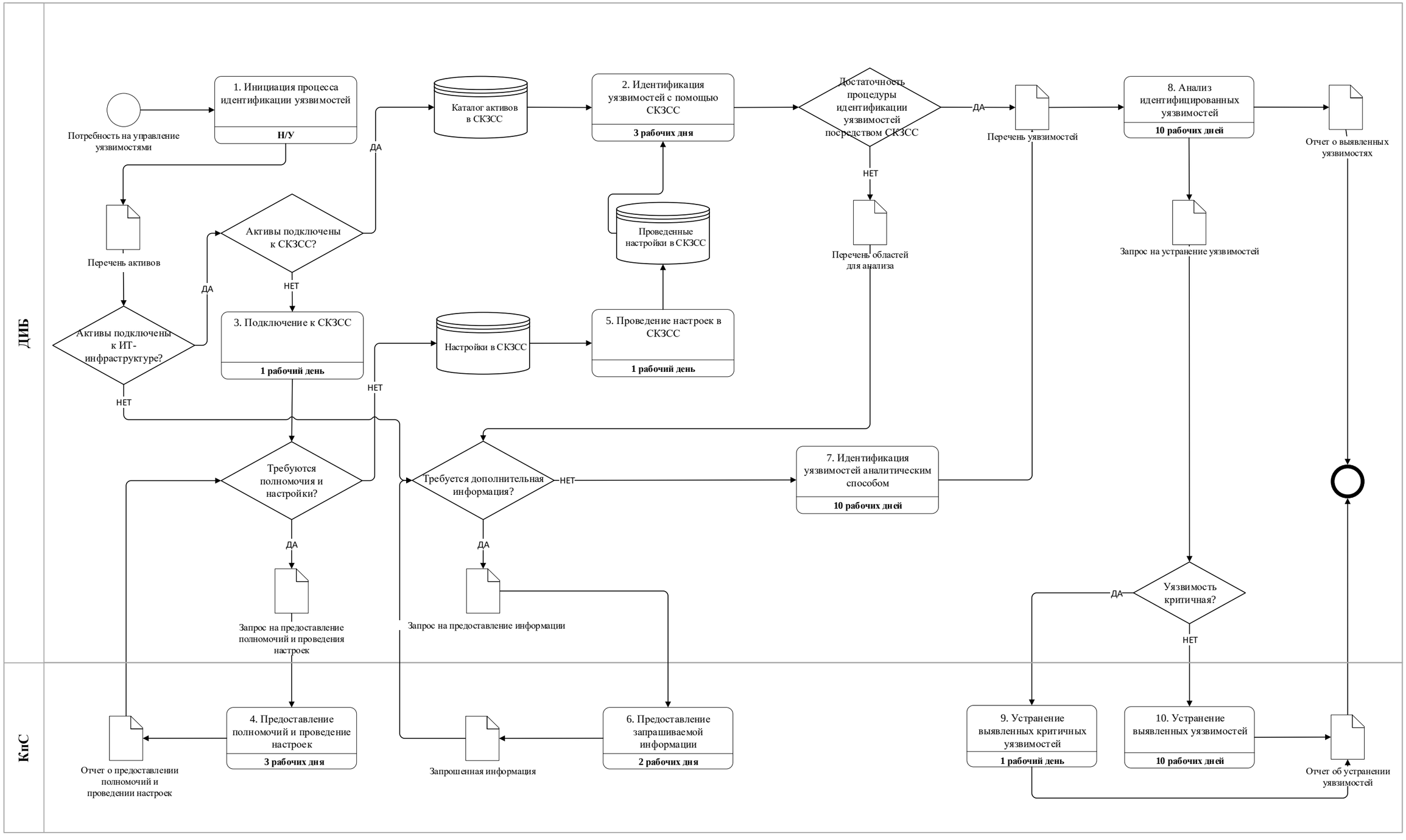
4.5 Для целей настоящего Регламента для подтверждения процедуры документирования операций и коммуникаций по Процессу равнозначными признаются:

– сообщения электронной почты с вложениями электронных документов в формате пакета приложений Microsoft Office версии 2013 и выше.
– служебные записки в корпоративной системе электронного документооборота с вложениями электронных документов в формате пакета приложений Microsoft Office версии 2013 и выше.

4.6 Целевое состояние Процесса: получение информации об уязвимостях всех Активов, подключенных к информационной инфраструктуре ООО «Сатурн», в реальном времени.

4.7 Сотрудники КпС, а также сотрудники иных структурных подразделений Корпорации обязаны информировать о всех идентифицированных ими уязвимостях Директора по эксплуатации систем информационной безопасности.

5. Блок-схема Процесса



6. Описание Процесса

№	Операция	Ответственный	Срок	Входящие документы	Детальное описание операции	Исходящие документы
1	2	3	4	5	6	7
1.	Инициация процесса идентификации уязвимостей	Директор по эксплуатации систем информационной безопасности	Не применимо	1. Потребность в процессе идентификации и анализа уязвимостей в рамках моделирования угроз ИБ и оценки рисков ИБ 2. Постоянный мониторинг уязвимостей 3. Информация об уязвимостях из внешней среды (внешние источники информации, результаты тестов на проникновение)	Потребность в Процессе возникает в следующих случаях: – При обнаружении изменений в информационной инфраструктуре включая обнаружение новых активов в инфраструктуре или состава и конфигурации известных Активов; – Для процесса моделирования угроз и оценки рисков; – На стадии планирования, создания и разработки/внедрения активов – Проверка эффективности в рамках тестирования на проникновение – В рамках постоянной оценки защищенности Активов. На указанном этапе работником ДИБ определяется, подключен ли Актив к информационной инфраструктуре и возможности по применению СКЗСС для идентификации уязвимостей. В случае если интересуемые Активы подключены к информационной инфраструктуре ООО «Сатурн», но не подключены к СКЗСС, работник ДИБ должен инициировать подключение Актива к СКЗСС. В случае если Активы не подключены к информационной инфраструктуре, что бывает обычно в случае если Актив планируется к внедрению (разработке или находится на стадии планирования или проектирования) или полученных данных об уязвимостях на предыдущем этапе недостаточно для идентификации всех уязвимостей работник ДИБ должен собрать всю необходимую для идентификации и последующего анализа уязвимостей информацию, включая направление запроса на предоставление информации сотрудникам КпС в зависимости от принадлежности Активов.	1. Перечень Активов 2. Запрос на предоставление информации

№	Операция	Ответственный	Срок	Входящие документы	Детальное описание операции	Исходящие документы
1	2	3	4	5	6	7
2.	Идентификация уязвимостей с помощью СКЗСС	Работник ДИБ в соответствии с должностной инструкцией	3 рабочих дня	1. Каталог Активов СКЗСС 2. Проведенные настройки в СКЗСС	Для Активов, подключенных к СКЗСС, настраивается частота и период проведения сканирования Активов на уязвимости. Работники ДИБ, которым предоставлен доступ к СКЗСС, могут производить внеплановые сканирования Активов на уязвимости. Частота и период проведения сканирования определяется техническими возможностями и критичностью Активов и фиксируется настройками СКЗСС на основании решения Директора по эксплуатации систем информационной безопасности. В случае если проведенного сканирования посредством СКЗСС недостаточно для идентификации всех уязвимостей работник ДИБ должен запрашивать дополнительную информацию об Активах и проводить дальнейшую идентификацию уязвимостей аналитическим способом или с применением других имеющихся в его наличии программных и технических средств.	1. Перечень уязвимостей 2. Перечень областей для анализа
3.	Подключение к СКЗСС	Работник ДИБ в соответствии с должностной инструкцией	1 рабочий день	1. Перечень Активов	Для подключения Активов к СКЗСС работник ДИБ проводит оценку и проверку достаточности полномочий в СКЗСС и технической доступности (поддержку сканирования в СКЗСС) для сканирования Актива и подготавливает настройки для СКЗСС (включая обновление каталога Активов в СКЗСС). В случае недостаточности полномочий или технической доступности для сканирования посредством СКЗСС Активов работник ДИБ оформляет запрос на предоставление полномочий и проведения настроек и направляет его в Директору по инфраструктуре, с копией Директору по эксплуатации систем информационной безопасности. Тестирует и подтверждает возможности СКЗСС по проведению идентификации уязвимостей. В случае не прохождения проверки работник ДИБ оформляет новый запрос на предоставление полномочий и проведения настроек.	1. Запрос на предоставление полномочий и проведения настроек 2. Настройки в СКЗСС

№	Операция	Ответственный	Срок	Входящие документы	Детальное описание операции	Исходящие документы
1	2	3	4	5	6	7
4.	Предоставление полномочий и проведение настроек	Директор по инфраструктуре	3 рабочих дня	1. Запрос на предоставление полномочий и проведения настроек	На основании запроса на предоставление полномочий и проведения настроек Директор по инфраструктуре проводит необходимые изменения и предоставляет необходимые полномочия и по результатам обязан уведомить инициатора Запроса на предоставление полномочий и проведения настроек посредством направления ему соответствующего Отчета с обязательным указанием в копии Директора по эксплуатации систем информационной безопасности. В случае повторного Запроса на предоставление полномочий и проведения настроек срок выполнения указанного Запроса не может превышать 1 рабочего дня. По согласованию с Директором по эксплуатации систем информационной безопасности время предоставления информации может быть увеличено на необходимый срок.	1. Отчет о предоставлении полномочий и проведении настроек
5.	Проведение настроек в СКЗСС	Работник ДИБ в соответствии с должностной инструкцией	1 рабочий день	1. Отчет о предоставлении полномочий и проведении настроек	По результатам предоставления полномочий и проведения настроек работник ДИБ проводит настройки СКЗСС включая обновление каталога Активов в СКЗСС. По результатам проведения настроек в СКЗСС проводит идентификацию уязвимостей посредством СКЗСС	1. Проведенные настройки в СКЗСС
6.	Предоставление запрашиваемой информации	Директор по инфраструктуре	2 рабочих дня	1. Запрос на предоставление информации 2. Перечень активов	После поступления запроса от ДИБ на предоставление запрашиваемой информации Директор по инфраструктуре должен обеспечить направление запрошенной информации в зависимости от принадлежности Активов. В случае если в создании, разработке и внедрении Активов участвуют подрядные организации Директор по инфраструктуре имеет право организовать прямое взаимодействие ДИБ и ответственных от подрядной организации при сохранении сроков предоставления информации. В случае повторного Запроса на предоставление информации срок выполнения указанного Запроса не может превышать 1 рабочего дня. По согласованию с Директором по эксплуатации систем информационной безопасности время предоставления информации может быть увеличено на необходимый срок.	1. Запрошенная информация

№	Операция	Ответственный	Срок	Входящие документы	Детальное описание операции	Исходящие документы
1	2	3	4	5	6	7
7.	Идентификация уязвимостей аналитическим способом	Работник ДИБ в соответствии с должностной инструкцией	10 рабочих дней	1. Запрошенная информация 2. Перечень активов	Идентификация уязвимостей на данном этапе производится экспертным способом, посредством анализа состава, функционала и способов взаимодействия (и других аспектов функционирования) Активов на основании всей собранной информации. Работник ДИБ определяет полноту предоставленной информации. Отсутствие требуемой работнику ДИБ информации не позволяет произвести идентификацию уязвимостей. По согласованию с Директором по эксплуатации систем информационной безопасности срок проведения идентификации уязвимостей может быть продлен. Указанный способ является единственным для выявления архитектурных и организационных уязвимостей.	1. Перечень уязвимостей
8.	Анализ идентифицированных уязвимостей	Работник ДИБ в соответствии с должностной инструкцией	10 рабочих дней	1. Перечень уязвимостей	По результатам полученного Перечня выявленных уязвимостей для Активов, ДИБ проводит оценку их критичности. По результатам анализа работник ДИБ готовит отчет о выявленных уязвимостях и запрос на устранение уязвимостей. Критичность выявленных уязвимостей после проведения их анализа определяется ДИБ, информация о них особо выделяется в Отчете о выявленных уязвимостях и в Запросе на устранение уязвимостей направляемом Директору по инфраструктуре в зависимости от принадлежности уязвимых Активов.	1. Отчет о выявленных уязвимостях 2. Запрос на устранение уязвимостей

№	Операция	Ответственный	Срок	Входящие документы	Детальное описание операции	Исходящие документы
1	2	3	4	5	6	7
9.	Устранение выявленных критических уязвимостей	Директор по инфраструктуре	1 рабочий день	1. Запрос на устранение уязвимостей	В случае получения запроса на устранение уязвимостей в котором ДИБ определены критические уязвимости, Директор по инфраструктуре должен в течении 1 рабочего дня произвести устранение выявленных критичных уязвимостей. В случае невозможности устранения выявленных критичных уязвимостей в установленные Регламентом сроки, Директор по инфраструктуре должен предоставить Директору по эксплуатации систем информационной безопасности детальные технические обоснования о невозможности устранения уязвимостей в установленные Регламентом сроки и согласовать с Директором по информационной безопасности срок устранения уязвимостей. Устранение уязвимостей может происходить посредством установки новой версии программного обеспечения (при её наличии), в котором подтверждено устранение уязвимостей разработчиком или производителем Актива, или отключением уязвимого функционала (подсистем или его частей). Для Активов планируемых к внедрению и еще не подключенных к информационной инфраструктуре ООО «Сатурн» не должно существовать критичных уязвимостей.	1. Отчет об устраненных уязвимостях
10.	Устранение выявленных уязвимостей	Директор по инфраструктуре	10 рабочих дней	1. Запрос на устранение уязвимостей	При получении запроса на устранении уязвимостей в котором не выявлены критические уязвимости, или в котором критические уязвимости присутствуют совместно с не критическими Директор по инфраструктуре должен в течение 10 рабочих дней произвести устранение выявленных некритических уязвимостей. Устранение уязвимостей может происходить посредством установки новой версии программного обеспечения (при её наличии), в котором подтверждено устранение уязвимостей разработчиков или производителем Актива, или отключением уязвимого функционала (подсистем или его частей). В случае невозможности устранения выявленных критичных уязвимостей в установленные Регламентом сроки, Директор по инфраструктуре должен предоставить Директору по эксплуатации систем информационной безопасности детальные технические обоснования о невозможности устранения уязвимостей в установленные Регламентом сроки срок и согласовать с Директором по эксплуатации систем информационной безопасности срок устранения уязвимостей.	1. Отчет об устраненных уязвимостях

7. Порядок пересмотра Регламента

7.1 При возникновении необходимости в Регламент вносятся изменения.

7.2 Инициатором внесения изменений в Регламент может быть любое структурное подразделение ООО «Сатурн», путем направления служебной записки на имя Директора по эксплуатации систем информационной безопасности с обоснованием необходимости пересмотра Регламента.

8. Контроль

8.1 Контроль за соблюдением положений Регламента осуществляется ДИБ.

8.2 В рамках проведения процедур идентификации и анализа уязвимостей информационной безопасности работники ДИБ имеют право применять все необходимые программные и технические средства включая те, на которые установлен запрет другими локальными нормативными актами ООО «Сатурн».

8.3 С целью контроля за эффективностью процесса управления уязвимостями информационной безопасности не реже 1 раза в год должен проводится независимый тест на проникновение.

8.4 ДИБ в случае обнаружения фактов нарушения положений Регламента, возникших в связи с недобросовестным исполнением Участниками Процесса своих обязанностей в рамках Регламента или возникших в результате нарушения нормативных документов ООО «Сатурн» в области информационной безопасности, сообщает о данных фактах вышестоящему руководителю сотрудника, нарушившего положения Регламента.

9. Ответственность

9.1 Участники процесса управления уязвимостями информационной безопасности ООО «Сатурн» несут персональную ответственность за соблюдение положений Регламента.

9.2 К работникам, нарушившим положения Регламента могут применяться дисциплинарные взыскания в порядке, установленном законодательством Российской Федерации.

9.3 Ответственность третьих лиц, включая сотрудников подрядных организаций, должны учитываться в договорах (соглашениях), заключенных с ними. Ответственность за включение положений настоящего Регламента лежит на кураторе договора.