УТВЕРЖДАЮ:

«__» _____ 20__ г.

СТО № ИБ.003

Регламент управления рисками 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 4

2. Нормативные ссылки 4

3. Термины и сокращения 5

4. Общие положения 6

5. Блок-схема Процесса 7

6. Описание Процесса 8

7. Порядок пересмотра Регламента 12

8. Контроль 12

9. Ответственность 12

Приложение № 1 13

Приложение № 2 15

1. Цель и область действия

1.1 Цель Регламента

Целью разработки Регламента управления рисками информационной безопасности ООО «Сатурн» (далее – Регламент) является повышение уровня информационной безопасности ООО «Сатурн», а также подтверждение того, что Корпорация своевременно и эффективно реагирует на угрозы информационной безопасности.

1.2 Область действия

1.2.1 Потребность в реализации процесса:

1.2.1.1 Выстраивание системы управления информационной безопасности, обеспечивающей своевременное и эффективное отражение существующих и новых угроз информационной безопасности для Корпорации.

1.2.1.2 Предоставление отчетности в рамках корпоративной системы управления рисками.

1.2.2 Результаты выполнения процесса:

1.2.2.1 Перечень рисков информационной безопасности для Активов ООО «Сатурн».

1.2.2.2 Отчет о рисках ИБ.

1.2.2.3 План обработки рисков ИБ.

1.2.3 Настоящий Регламент:

1.2.3.1 Определяет системный подход к процессу управления рисками информационной безопасности ООО «Сатурн». Системный подход к управлению рисками ИБ необходим для того, чтобы идентифицировать потребности Корпорации, касающиеся требований ИБ, и создать эффективную систему управления и обеспечения ИБ. Этот подход должен соответствовать условиям деятельности Корпорации. Усилия по обеспечению безопасности должны обеспечивать эффективное и своевременное реагирование на риски ИБ. Процесс управления рисками ИБ должен быть неотъемлемой частью всех бизнес-процессов Корпорации, связанных или зависимых от информационных технологий, и должен применяться как на этапе внедрения новых Активов, так и в процессе их эксплуатации и повседневного использования.

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

1.2.3.3 Определяет методику оценки рисков ИБ.

1.2.3.4 Предназначен для:

- Владельцев бизнес-процессов Корпорации.
- Владельцев Активов Корпорации.
- Руководителей СП Корпорации.
- Дирекции по информационной безопасности.

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 ИСО/МЭК 27001-2006. Национальный стандарт Российской Федерации. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

2.2 ГОСТ Р ИСО/МЭК 27005-2010. Национальный стандарт Российской Федерации. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Менеджмент риска информационной безопасности.

2.3 СТО № ИБ.002. Регламент управления уязвимостями информационной безопасности ООО «Сатурн»

2.4 СТО № ИБ.001. Методика моделирования угроз информационной безопасности ООО «Сатурн»

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 СП – Структурные подразделения Корпорации

3.2 В настоящем Регламенте использованы следующие термины:

3.2.1 Активы ООО «Сатурн» – информация, данные, 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 КпС ООО «Сатурн». Следует учитывать, что владельцами данных и информации в большинстве случаев являются структурные подразделения Корпорации, КпС обеспечивает сервисы хранения, обработки и передачи указанных данных и информации.

3.2.2 Влияние (последствия, ущерб) – воздействие на Активы, выраженное в негативных (неблагоприятных) последствиях для Корпорации или в прямом финансовом, экономическом, репутационном и других типах ущерба. В контексте Регламента идентично терминам последствия и ущерб от реализации угроз ИБ.

3.2.3 Идентификация риска – процесс нахождения, составления перечня и описания элементов риска.

3.2.4 Минимизация риска – действия направленные, на снижение возможного Влияния на Активы.

3.2.5 Количественная оценка риска – процесс присвоения значений вероятности и последствий риска.

3.2.6 Перенос риска – разделение ответственности бремени потерь или выгод от риска с третьими лицами. В частности, типичным примером переноса рисков является страхование рисков.

3.2.7 Предотвращение риска – принятие решение не быть вовлеченным в рискованную ситуацию или процедуру, отказ от решений, ведущих к возникновению рисков.

3.2.8 Процесс – процесс управления рисками информационной безопасности.

3.2.9 Риск информационной безопасности – возможность того, что угроза сможет воспользоваться уязвимостью Актива и тем самым нанесет ущерб Корпорации.

3.2.10 Снижение риска – действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском.

3.2.11 Сохранение (принятие) риска – принятие бремени потерь или выгод от конкретного риска.

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

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

3.2.14 Участники Процесса – СП Корпорации.

4. Общие положения

4.1 Процесс управления рисками является неотъемлемой частью системы управления информационной безопасностью.

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

4.2.1 Идентификация рисков.

4.2.2 Анализ и оценка рисков.

4.2.3 Обработка рисков.

4.3 Для повышения оперативности и эффективности Процесса, все проводимые в рамках исполнения положений Регламента коммуникации и операции, должны документироваться в электронном виде.

4.4 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.

4.5 Целевое состояние Процесса: обеспечение возможности получения информации о рисках для всех Активов, подключенных к информационной инфраструктуре ООО «Сатурн», в реальном времени с помощью специализированных решений по автоматизации управления рисками информационной безопасности.

4.6 Руководители СП, владельцы бизнес-процессов и Активов (информационных ресурсов) должны предоставлять информацию об оценке Влияния на Активы в их зоне ответственности, а также на Активы, от которых зависят бизнес-процессы Корпорации, Владельцами которых они являются, в сроки, установленные отдельными приказами и распоряжениями, Директору по эксплуатации систем информационной безопасности в соответствии с Приложениями № 1 и № 2 к Регламенту.

4.7 Дирекция по информационной безопасности является центром компетенции по указанным далее областям знаний и методик и не обязан предоставлять дополнительных разъяснений или подтверждений:

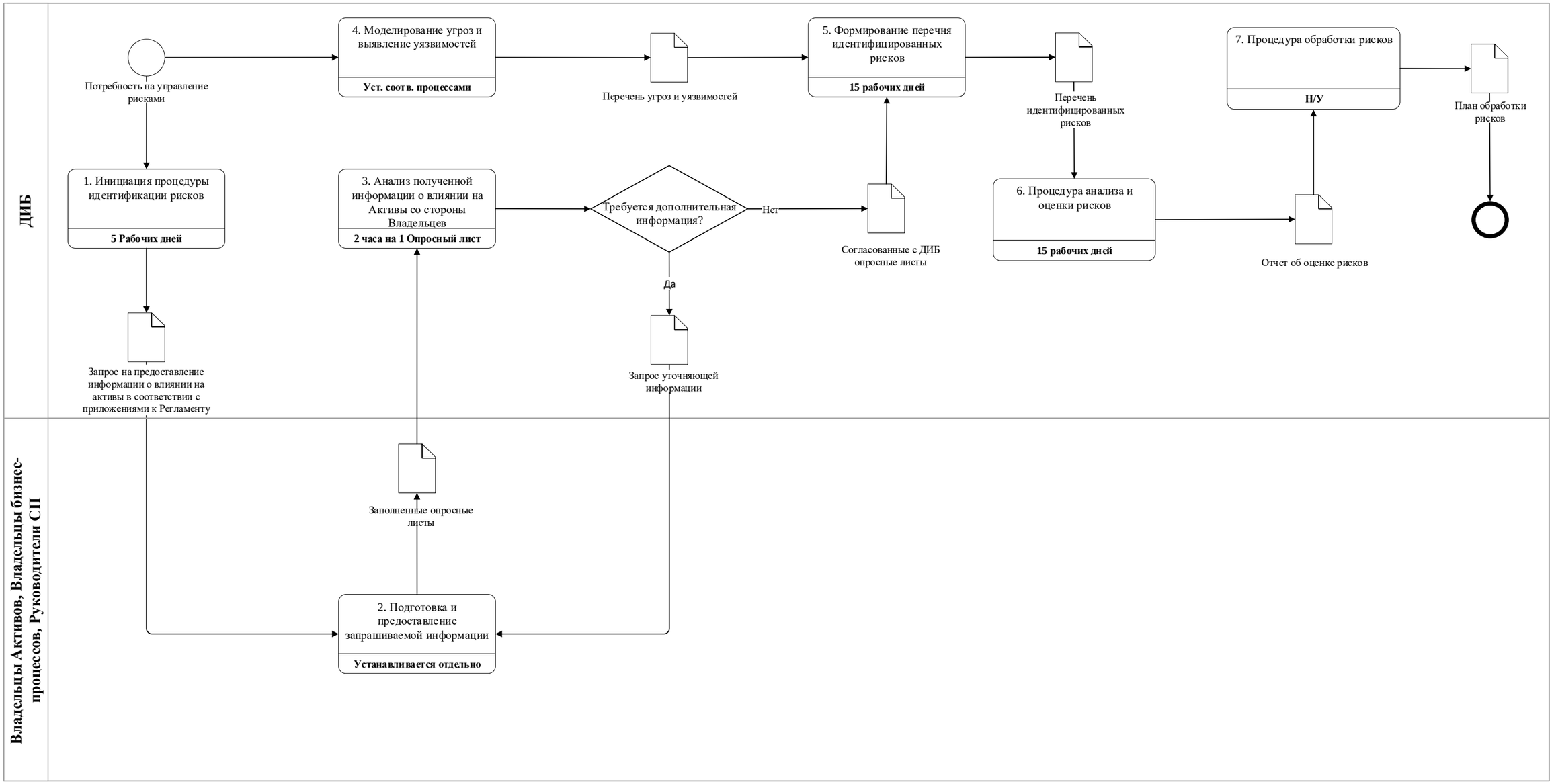
- по определению вероятности наступления событий, связанных с реализацией угроз информационной безопасности;
- по определению потенциала и наличия ресурсов у злоумышленника;
- по определению возможности эксплуатации уязвимостей информационной безопасности.

4.8 С целью адекватной оценки угроз информационной безопасности все СП Корпорации должны информировать Директора по эксплуатации систем информационной безопасности обо всех потенциальных негативных внешних факторах для Корпорации, возникающих в связи с применением ими информационных технологий, не позднее 3 рабочих дней со дня их обнаружения.

4.9 Ответственные работники КпС дополнительно обязаны в рамках п.4.6 Регламента предоставлять информацию о стоимости Активов, являющейся совокупностью затрат на создание, внедрение и эксплуатацию указанных Активов.

4.10 Риски ИБ должны пересматриваться не реже 1-го раза в год.

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 рисков	Директор по эксплуатации систем информационной безопасности	5 рабочих дней после принятия решения о старте процедуры	1. Потребность в процессе идентификации и анализа уязвимостей в рамках моделирования угроз ИБ и оценки рисков ИБ 2. Перечень Активов	Потребность в Процессе возникает в следующих случаях: – При изменении состава, характеристик и перечня Активов или условий его существования; – Ежеквартальная сдача отчетности по рискам в рамках корпоративной системы управления рисками; – Для процесса моделирования угроз и оценки рисков; – На стадии планирования, создания и разработки/внедрения Активов – Запрос на предоставление информации о рисках со стороны руководства Корпорации. – Появление новых угроз информационной безопасности. – Значительное ухудшение состояния защищенности активов определяется в рамках процесса управления уязвимостями Дирекция по информационной безопасности при появлении потребности в оценке рисков готовит приказ или распоряжение по Корпорации с указанием Активов в отношении которых будет проводится оценка, в рамках выпускаемого приказа или распоряжения указываются Владельцы Активов, которые в соответствии с Регламентом должны будут предоставить/актуализировать информацию в соответствии с опросными листами (Приложение № 1 и № 2 к Регламенту). Параллельно в рамках процесса управления уязвимостями и методикой моделирования угроз информационной безопасности ДИБ готовит соответствующую информацию по возможности осуществления негативного воздействия на Активы.	Запрос на предоставление информации о влиянии на активы в соответствии с приложениями к Регламенту

№	Операция	Ответственный	Срок	Входящие документы	Детальное описание операции	Исходящие документы
1	2	3	4	5	6	7
2.	Подготовка и предоставление запрашиваемой информации	Владельцы Активов, Владельцы бизнес-процессов, Руководители СП	Устанавливается посредством отдельного Приказа/ Распоряжения	1. Запрос на предоставление информации о влиянии на активы в соответствии с приложениями к Регламенту 2. Запрос уточняющей информации	Владельцы Активов, Владельцы бизнес-процессов, Руководители СП заполняют опросные листы в соответствии с Приложениями № 1 и № 2 к Регламенту. В рамках данного этапа ответственные работники КпС дополнительно обязан предоставить информацию о стоимости Активов, являющейся совокупностью затрат на создание, внедрение и эксплуатацию указанных Активов.	Заполненные опросные листы в соответствии с Приложениями № 1 и № 2 к Регламенту
3.	Анализ полученной информации о влиянии на Активы со стороны Владельцев	Директор по эксплуатации систем информационной безопасности	2 часа на 1 опросный лист	1. Заполненные опросные листы в соответствии с Приложениями № 1 и № 2 к Регламенту	В рамках анализа полученных заполненных опросных листов могут потребоваться уточнение и консультационные совещания с Владельцами Активов, Владельцами бизнес-процессов, Руководителями СП. Результатом данного этапа является определение Влияния на Активы, определяемого Владельцами Активов, Владельцами бизнес-процессов, Руководителями СП согласованного с непосредственными руководителями и ДИБ.	1. Согласованные с ДИБ опросные листы 2. Запрос уточняющей информации
4.	Моделирование угроз и выявление уязвимостей	Директор по эксплуатации систем информационной безопасности	Устанавливается в рамках соответствующих методики моделирования угроз и регламента управления уязвимостями ИБ	1. Потребность в процессе идентификации и анализа уязвимостей в рамках моделирования угроз ИБ и оценки рисков ИБ 2. Перечень Активов	ДИБ для перечня Активов, попавших в область оценки рисков определяет угрозы и уязвимости информационной безопасности.	Перечень угроз и уязвимостей
5.	Формирование перечня идентифицированных рисков	Директор по эксплуатации систем информационной безопасности	15 рабочих дней	1. Согласованные с ДИБ опросные листы 2. Перечень угроз и уязвимостей	На основании полученного перечня угроз и уязвимостей для Активов, попавших в область оценки и возможного Влияния (Критичности) на Активы формируется итоговый перечень идентифицированных рисков ИБ.	Перечень идентифицированных рисков

№	Операция	Ответственный	Срок	Входящие документы	Детальное описание операции	Исходящие документы
1	2	3	4	5	6	7
6.	Процедура анализа и оценки рисков	Директор по эксплуатации систем информационной безопасности	15 рабочих дней	Перечень идентифицированных рисков	На основании итогового перечня идентифицированных рисков проводится анализ рисков. По результатам которого риски ИБ классифицируются по критичности и ущербу. При этом ущерб может характеризоваться: – Финансовыми потерями; – Нарушением законодательства и других нормативно-правовых актов, условий договоров и т.п.; – Репутационными потерями; – Физическими потерями. Результаты анализа рисков ИБ оформляются в виде отчета или в рамках отчетности по КСУР в зависимости от исходного запроса. В отчете указываются различные варианты обработки рисков, а также при необходимости планы обработки рисков. Отчет в зависимости от принадлежности Активов, наличия возможности принятия адекватных мер может выносится на различные уровни принятия решений (Комитет по рискам, Совещания с генеральным директором) в которых определяется механизм обработки риска: – Принятие риска; – Предотвращение риска; – Минимизация риска; – Перенос (страхование) риска; В случае выбора механизмов предотвращения и минимизации рисков может потребоваться дополнительное финансирование соответствующих мероприятий. Согласование дополнительного финансирования должно происходить в рамках принятия решений по выбору механизма обработки выявленных рисков. При отсутствии необходимости дополнительного финансирования процедур обработки рисков ИБ, связанных с предотвращением рисков ИБ или их минимизацией, Директор по эксплуатации систем информационной безопасности самостоятельно вырабатывает указанные механизмы в рамках системы управления и обеспечения информационной безопасности При необходимости может быть инициирована процедура принятия риска на уровне Генерального директора (по результатам обсуждения)	Отчет об оценке рисков

№	Операция	Ответственный	Срок	Входящие документы	Детальное описание операции	Исходящие документы
1	2	3	4	5	6	7
7.	Процедура обработки рисков	Директор по эксплуатации систем информационной безопасности	Не установлено	Отчет об оценке рисков	ДИБ по результатам утверждения отчета об оценке рисков ИБ и выборе механизмов обработки рисков формирует и реализует план обработки рисков. После реализации Плана обработки рисков требуется в зависимости от изменения внешних условий провести повторную процедуру оценки рисков.	План обработки рисков

7. Порядок пересмотра Регламента

7.1 При возникновении необходимости в Регламент вносятся изменения.

7.2 Пересмотр положений регламента производится ДИБ не реже одного раза в год.

7.3 Инициатором внесения изменений в Регламент может быть любое структурное подразделение ООО «Сатурн», путем направления служебной записки на имя Вице-президента – руководителя Департамента безопасности с обоснованием необходимости пересмотра Регламента.

8. Контроль

8.1 Контроль за соблюдением положений Регламента осуществляется ДИБ.

8.2 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 несут персональную ответственность за соблюдение положений Регламента:

9.1.1 Владельцы Активов, бизнес-процессов, руководители СП Корпорации несут ответственность за корректное предоставление данных по оценке стоимости Активов и Влиянию на Активы.

9.1.2 ДИБ несет ответственность за корректность и полноту процедуры выявления угроз и уязвимостей информационной безопасности для Активов.

Опросный лист об оценке параметров информационного ресурса (ИТ-актив) (Образец заполнения)	
Общие сведения об информационном ресурсе (ИТ-активе)	
Наименование информационного ресурса:	*Система контроля за утечками данных*
Краткое наименование информационного ресурса:	*DLP (Websense)*
Описание ресурса:	*Система предназначена для контроля пересылаемой информации ограниченного распространения*
Тип информационного ресурса:	*Автоматизированная система (Сетевая папка, локальная папка, раздел на корпоративном ресурсе, модуль в автоматизированной системе и другое)*
Заказчик информационного ресурса:	*Будников Александр Юрьевич*
Владелец информационного ресурса:	*Зайцев Алексей Андреевич*
Бизнес-процессы которые зависят от информационного ресурса:	*Управление информационной безопасностью*
Подразделения, работающие с информационным ресурсом:	*Департамент безопасности*
Обеспечивает реализацию внутренних или организационно-распорядительных документов и нормативных документов Корпорации:	*Кодекс «Безопасность», утвержденный Приказом ООО «Сатурн» от 22.06.2015 №У-039/15*
Используется ли информация для передачи вне Корпорации:	*Детально описать зависит ли какая-либо отчетность Корпорации от информационного ресурс, кому направляется, дублируется ли в неэлектронном виде (или не в информационных ресурсах Корпорации) и в какой мере*
Контактные данные лица ответственного за заполнение опросного листа:	
ФИО:	*Зайцев Алексей Андреевич*
Полное наименование должности	*Директор по эксплуатации систем информационной безопасности*
Адрес электронной почты	*a.zaytsev@sistema.ru*
Рабочий телефон	*50390*
Требования к конфиденциальности	
Обрабатываются персональные данные:	*Обрабатывается персональные данные работников Корпорации и ДЗК (Описать перечень персональных данных)*
Обрабатывается информация, составляющая коммерческую тайну Корпорации:	*Обрабатывается коммерческая тайна Корпорации (Описать состав сведений)*
Обрабатывается инсайдерская информация:	*Обрабатывается инсайдерская информация Корпорация*
Последствия нарушения конфиденциальности:	*В соответствии с ФЗ «О персональных данных» Снижение уровня информационной безопасности и защищенности информационных ресурсов Оценивается в финансовых потерях, для Корпорации (или штрафы или упущенные доходы, административная или уголовная ответственность) при невозможности оцениваются репутационные риски и прочие. Необходимо исходить из результатов ответа на вопрос: "Что будет если информация будет опубликована в СМИ и сети Интернет"*
Требования к целостности	

Необходимо ли обеспечение контроля за изменением информации и гарантированного определения авторства:	*Да, необходимо регистрация действий всех пользователей и администраторов*
Последствия нарушения целостности:	*В указанном поле заполняется сведения о возможных последствиях для бизнес-процессов и/или Корпорации в случае несанкционированного изменения информации (подмены и подлога), возможно ли совершение мошеннических действий.* *Оценивается в финансовых потерях, для Корпорации (или штрафы или упущенные доходы, административная или уголовная ответственность)*
Подтверждаются ли действия в бумажном виде или еще в каких либо ресурсах:	*Указывается есть ли возможность гарантировано выявить факт подмены (подлога) информации, в случае наличия возможности обнаружения факта подмены указывается обнаружение будет произведено автоматически в рамках последующих операций по бизнес-процессу не в электронном виде*
Требования к доступности	
Максимальное допустимое время недоступности (простоя, неработоспособности) системы (RTO):	*24 часа, указывается крайний случай (к примеру система используется 1 раз в квартал, и данные для некоторого отчета подаются в последний рабочий день квартала, то допустимое время простоя будет 4 часа при условии, что данные возможно обработать в течении 4 часов для подготовки отчета)*
Допустимое время потери данных (RPO):	*4 часа, необходимо понимать, что резервирование данных в системе не происходит в реальном времени и резервные копии, снимаются в среднем раз в сутки, раз в неделю, для критичных систем раз в час. При этом если произошёл сбой в системе для которой резервные копии снимаются раз в сутки то необходимо понимать, что будут утрачены все данные в системе начиная с момента последнего резервного копирования этим указанным периодом и является допустимое время потери данных*
Последствия недоступности и потери данных:	*Описываются последствия в случае неработоспособности системы в самом крайнем случае?* *Кроме того описываются последствия полной потери данных, и потери данных после RPO* *(Оценивается в финансовых потерях, для Корпорации (или штрафы или упущенные доходы, административная или уголовная ответственность)*
Дополнительные сведения	
Указываются любые другие сведения об информационном ресурсе, которые нельзя включить в предыдущие поля	

Заполненные опросные листы направляются на адрес электронной почты Директора по эксплуатации систем информационной безопасности. К письму прилагается выписка или полностью, копия положения о структурном подразделении как в формате Word, так и формате сканированной копии

Опросный лист об оценке влияния информационных технологий на деятельность структурного подразделения (образец заполнения)	
Общие сведения об информационном ресурсе (ИТ-активе)	
Полное наименование структурного подразделения:	*Дирекция по информационной безопасности Департамента безопасности*
Краткое наименование структурного подразделения:	*ДИБ*
Руководитель структурного подразделения:	*Управляющий Директор по информационной безопасности и специальным проектам Будников Александр Юрьевич*
Контактные данные лица, ответственного за заполнение опросного листа:	
ФИО:	*Зайцев Алексей Андреевич*
Полное наименование должности	*Директор по эксплуатации систем информационной безопасности*
Адрес электронной почты	*a.zaytsev@sistema.ru*
Рабочий телефон	*50390*
Использование информационных технологий структурным подразделением Корпорации	
Используемые для работы информационные ресурсы (ИТ-активы):	*Корпоративная электронная почта* *Автоматизированное рабочее место (компьютер)* *Телефонная связь* *Файловые ресурс* *СЭД* *Системы информационной безопасности*
Максимальный срок недоступности указанных информационных ресурсов (ИТ-активов):	*2 часа*
Последствия недоступности используемых информационных ресурсов:	*Полная остановка процесса обеспечения ИБ (Указывается для каждого вышеуказанного ресурса, подразумевается утрата указанного информационного ресурса (ИТ-актива) для всего структурного подразделения) (Оценивается в финансовых потерях, для Корпорации (или штрафы или упущенные доходы, административная или уголовная ответственность)*
Последствия утраты информации:	*Указывается если в подразделении были организованы свои локальные ресурсы хранения информации Оценивается в финансовых потерях, для Корпорации (или штрафы или упущенные доходы, административная или уголовная ответственность)*
Использование информационных технологий в разрезе взаимодействия с другими структурными подразделениями Корпорации	
По каждому пункту раздела о взаимоотношениях (служебных связях) Положения о структурном подразделении:	*Указывается получатель или отправитель из Положения о структурном подразделении, формат документов (данных и информации), предоставляемых или получаемых от других структурных подразделений (включая внешние организации), список используемых ресурсов для передачи, обработки и хранения указанных данных*
Взаимоотношение № 1	*Копируется из Положения о структурном подразделении, для примера:* *Для выполнения функций, предусмотренных настоящим Положением, Дирекция взаимодействует:* *8.1 Со всеми структурными подразделениями Корпорации:* *Дирекция получает:* *8.1.1 Информацию о подозрениях на нарушения информационной безопасности.*
Формат данных:	*Сообщение в электронном виде*
Какие информационные ресурсы (ИТ-активы)	*К примеру: Телефонная связь, электронная почта - передача информации, СЭД - обработка и хранение*

используются и с какой целью:	
Наличие резервных каналов обработки информации и взаимодействия:	*Например в бумажном виде с подписью, все документы складываются в архив*
Последствия нарушения конфиденциальности	*Оценивается в финансовых потерях, для Корпорации (или штрафы или упущенные доходы, административная или уголовная ответственность), а также репутационный и прочий ущерб*
Последствия несанкционированного изменения данных	*Оценивается в финансовых потерях, для Корпорации (или штрафы или упущенные доходы, административная или уголовная ответственность), в трудозатратах какие последствия для структурных других структурных подразделений, для самого структурного подразделения*
Последствия нарушения доступности	*Оценивается в финансовых потерях, для Корпорации (или штрафы или упущенные доходы, административная или уголовная ответственность), в трудозатратах какие последствия для структурных для других структурных подразделений, для самого структурного подразделения, в том числе оцениваются потери информации*
…	
Взаимоотношение № N	

Дополнительные сведения

Указываются любые другие сведения об используемых структурным подразделением информационных ресурсов (ИТ-активов), которые нельзя включить в предыдущие поля

Заполненные опросные листы направляются на адрес электронной Директора по эксплуатации систем информационной безопасности. К письму прилагается выписка или полностью, копия положения о структурном подразделении как в формате Word, так и формате сканированной копии