УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПОЛОЖЕНИЕ
О СВЕДЕНИЯХ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

[ИБ-104]

2018г.

1. Общие положения

1.1. Положение о сведениях конфиденциального характера (далее – Положение) разработано с целью защиты интересов ООО «Сатурн» (далее – Компания), путем обеспечения конфиденциальности.

1.2. Положение распространяется на все подразделения Компании.

1.3. В организационно-распорядительных документах Компании допускается для обозначения понятия «Сведения конфиденциального характера» применять термин «Конфиденциальная информация».

1.4. Настоящее Положение является локальным нормативным актом и разработано с учетом норм:

- Федерального закона от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне»;
- Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федерального закона от 30 декабря 2001 года № 197-ФЗ «Трудовой кодекс Российской Федерации»;
- Федерального закона от 18 декабря 2006 года № 230-ФЗ «Гражданский кодекс РФ. Часть четвертая»;
- Указа Президента Российской Федерации от 06.03.1997 года № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТРк), утвержденные 02.03.2001г. решением № 7.2 Коллегии Гостехкомиссии России при Президенте Российской Федерации;
- Положения «О коммерческой тайне»;
- Устава Компании.

1.5. Компания имеет исключительное право на использование сведений конфиденциального характера любыми законными способами по собственному усмотрению.

1.6. В соответствии с настоящим Положением Компания принимает меры по обеспечению защиты и охраны сведений конфиденциального характера и ограничению доступа к ней третьих лиц.

1.7. Действие настоящего Положения распространяется в порядке и на условиях, предусмотренных настоящим Положением на:

- работников Компании;
- физических и юридических лиц, осуществляющих правоотношения с Компанией на основе норм ГК РФ.

1.8. Положение является обязательным для выполнения всеми работниками Компании и устанавливает единый порядок работы со сведениями конфиденциального

характера.

1.9. Передача сведений конфиденциального характера как работникам Компании, так и третьим лицам, включая представителей контрагентов Компании и государственных органов, осуществляется исключительно в рамках исполнения трудовых обязанностей и с соблюдением требований, установленных законодательством РФ, настоящим Положением и другими действующими локальными нормативным актами Компании.

2. Определения и сокращения

В настоящем Положении применяются следующие определения и сокращения:

Работник – физическое лицо, вступившее в трудовые отношения с Компаниям на основании трудового договора и на иных основаниях, предусмотренных ст. 16 ТК РФ.

Доступ к информации – возможность получения информации.

Интеллектуальная собственность – особый вид собственности, имеющей виртуальный характер и нематериальную природу.

Информация – сведения (сообщения, данные) независимо от формы их представления

Коммерческая тайна – информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам

Объекты интеллектуальной собственности (общепринятое сокращение – интеллектуальная собственность) – оформленные документально результаты интеллектуальной деятельности человека (далее – РИД), соответствующие критериям, оговоренным в законодательстве

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)

Персональные данные работников – информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника

СВТ – средства вычислительной техники

Сведения конфиденциального характера (сведения ограниченного распространения, конфиденциальная информация) - сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях. Сведения, составляющие тайну следствия и судопроизводства. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна), а также действующими локальными нормативными актами Компании. Сведения, связанные с профессиональной деятельностью, доступ к которой ограничен в соответствии с Конституцией Российской Федерации и федеральными законами

(врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее), а также действующими локальными нормативными актами Компании. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна). Сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них.

Служебная тайна – информация ограниченного распространения, ставшая известной работникам в связи с исполнением ими должностных обязанностей

СТРк – Специальные требования и рекомендации по технической защите конфиденциальной информации

Разглашение сведений конфиденциального характера – любая передача работникам компании либо третьим лицам сведений конфиденциального характера, не обусловленная выполнением трудовых обязанностей и/или происходящая с нарушением требований законодательства РФ, настоящего Положения или других утвержденных локальных нормативных актов Компании.

3. Сведения конфиденциального характера Компании

3.1. К сведениям конфиденциального характера может относиться информация:

- о результатах интеллектуальной деятельности Компании;
- финансово-экономическая и плановая информация Компании;
- о способах и методах осуществления профессиональной деятельности;
- персональные данные работников и контрагентов Компании;
- об организационно-штатной структуре и размерах заработных плат работников;
- о принципах и методах организации систем безопасности объектов и защиты информации в Компании;
- иная информация о хозяйственной и производственной деятельности Компании не являющаяся общедоступной или к которой у третьих лиц нет свободного доступа на законном основании.

Перечень сведений конфиденциального характера Компании, приведен в Приложении 1.

4. Права Компании, как обладателя сведений конфиденциального характера

4.1. Обладателем сведений конфиденциального характера, полученных в рамках трудовых отношений, является Компания.

4.2. Компания имеет право:

- использовать сведения конфиденциального характера, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;
- разрешать или запрещать доступ к сведениям конфиденциального характера, определять порядок и условия доступа к этой информации;

- требовать от юридических лиц, физических лиц, получивших доступ к сведениям конфиденциального характера, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена конфиденциальная информация соблюдения обязанностей по охране её конфиденциальности;
- применять технические и иные средства для контроля соблюдения конфиденциальности сведений конфиденциального характера лицами, получившими доступ к этой информации;
- требовать от лиц, получивших доступ к сведениям конфиденциального характера, в результате действий, совершённых случайно или по ошибке, охраны конфиденциальности этой информации;
- защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами сведениям конфиденциального характера, в том числе требовать возмещения убытков, причинённых в связи с нарушением её прав.

4.3. В случае получения работником Компании, в связи с выполнением трудовых обязанностей или конкретного задания Компании, результата, способного к правовой охране в качестве изобретения, полезной модели, промышленного образца, программы для электронных вычислительных машин или базы данных, отношения между работником и Компанией регулируются в соответствии с «Гражданским Кодексом Российской Федерации» и действующими в Компании ЛНА.

5. Порядок отнесения информации к сведениям конфиденциального характера

5.1. Право на отнесение информации к сведениям конфиденциального характера, определение перечней и состава такой информации принадлежит Компании в соответствии с нормами Федерального законодательства, указанными в пункте 1.4 раздела 1 настоящего Положения.

5.2. Отнесение информации к сведениям конфиденциального характера осуществляется Генеральным директором Компании по представлению директоров департаментов, в соответствии с принципами обоснованности и своевременности. Обоснованность заключается в установлении целесообразности отнесения конкретных сведений к конфиденциальной информации. Своевременность заключается в установлении ограничений на разглашение этих сведений с момента их получения (разработки) или заблаговременно до указанного момента.

5.3. После принятия решения об отнесении информации к сведениям конфиденциального характера, последние вносятся в Перечень.

6. Обеспечение защиты и охраны сведений конфиденциального характера, в рамках трудовых отношений

6.1. В целях обеспечения безопасности и охраны сведений конфиденциального характера, Компания обязана:

- ознакомить работника с перечнем сведений конфиденциального характера и действующими ЛНА;
- создать работнику необходимые условия для обеспечения конфиденциальности полученной им в рамках выполнения трудовых обязанностей информации.

6.2. В целях обеспечения конфиденциальности сведений конфиденциального характера, работник обязан:

- не разглашать сведения конфиденциального характера, обладателем которых является Компания и его контрагенты, и без их согласия не использовать эти сведения в личных целях в течение всего срока действия трудового договора и после прекращения его действия;
- сообщать Заместителю генерального директора по безопасности Компании о всех попытках посторонних лиц получить сведения конфиденциального характера;
- сообщать Заместителю генерального директора по безопасности Компании о всех случаях пропажи документов и носителей сведений конфиденциального характера, а также о фактах пропажи печатей, пропусков и ключей доступа к СВТ;
- немедленно сообщать Заместителю генерального директора по безопасности Компании о фактах распространения сведений конфиденциального характера, ставших известными работнику;
- передать Компании при прекращении или расторжении трудового договора материальные носители, имеющиеся в пользовании работника и содержащие сведения конфиденциального характера.

6.3. Компания вправе потребовать возмещения убытков, причинённых ей разглашением сведений конфиденциального характера, от лица, получившего доступ к этим сведениям в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем.

7. Защита сведений конфиденциального характера

7.1. Защита сведений конфиденциального характера при их обработке с использованием СВТ:

7.1.1. Защита конфиденциальной информации при обработке её в средствах вычислительной техники, обеспечивается внедрением комплекса организационно-технических мероприятий, программных средств, программно-аппаратных комплексов защиты и направлена на предотвращение:

- утечки информации по техническим (приём, хранение, передача) каналам;
- несанкционированного доступа к обрабатываемой и хранимой конфиденциальной информации;
- несанкционированного распространения конфиденциальной информации;
- программно-технического воздействия, представляющего угрозу безопасности конфиденциальной информации.

7.1.2. Непосредственное руководство работой по защите сведений конфиденциального характера при обработке на СВТ осуществляют руководители подразделений.

7.1.3. Контроль за обеспечением защиты конфиденциальной информации при её обработке на СВТ осуществляет подразделение по защите информации.

7.1.4. Обязательными условиями при обработке сведений конфиденциального характера, в СВТ являются:

- допуск пользователя к работе с СВТ путём использования индивидуальных учётных записей и паролей, смена которых производится не реже одного раза в квартал;
- возможность идентификации всех лиц в момент их обращения к информации;
- создание резервных копий программ и информационных массивов.

7.1.5. Основным критерием, определяющим уровень требований к средствам защиты информации, является степень конфиденциальности сведений, циркулирующих в информационной системе.

7.1.6. Средства обеспечения безопасности информации должны выбираться с учётом особенностей, связанных с режимами эксплуатации электронно-вычислительных систем и существующими возможностями преодоления защиты информации в используемой операционной среде.

7.1.7. Обмен информацией между пользователями, а также доставка её конечному потребителю могут быть осуществлены путём использования физических носителей информации (при автономной эксплуатации СВТ), соединительных кабелей (в локальных вычислительных сетях) и телекоммуникационных каналов связей (при передаче информации на значительные расстояния). Каждому способу передачи данных должны соответствовать требования защиты, учитывающие особенности транспортировки информации.

7.1.8. Организация хранения и эксплуатации электронных носителей сведений конфиденциального характера, а также определение порядка ремонта вычислительной техники возлагаются на руководителя направления ИТ Компании.

7.2. Защита сведений конфиденциального характера при обсуждении конфиденциальных вопросов и ведении переговоров:

- В целях обеспечения безопасности сведений конфиденциального характера при обсуждении конфиденциальных вопросов и ведении переговоров в Компании организуются защищаемые помещения. В соответствии с требованиями СТРк защищаемые помещения подлежат аттестации на соответствие требованиям по безопасности.
- Решение об оборудовании помещений, не являющихся защищаемыми, дополнительной охранной сигнализацией и постановки его под охрану в нерабочее время определяется руководителем самостоятельного структурного подразделения.

7.3. При утрате документов и носителей, содержащих сведения конфиденциального

характера, а также ключей от помещений с СВТ, сейфов и металлических шкафов, используемых для хранения носителей и распечатанных документов, работник, обнаруживший утрату, обязан незамедлительно поставить в известность руководителя направления безопасности и руководителя структурного подразделения.

8. Ответственность за разглашение сведений конфиденциального характера

8.1. Нарушение обязательств о неразглашении сведений конфиденциального характера влечёт за собой наложение на работников Компании дисциплинарной ответственности, в соответствии с Трудовым кодексом Российской Федерации.

8.2. Работник, который в связи с исполнением трудовых обязанностей получил доступ к сведениям конфиденциального характера, обладателями которой являются Компания, как работодатель, и его контрагенты, в случае умышленного или неосторожного разглашения таких сведений, может быть привлечен к гражданской, административной и уголовной ответственности в соответствии с законодательством Российской Федерации.

9. Заключительные положения

9.1. Внесение изменений и дополнений в соответствующие Перечни, допускается только в письменной форме и утверждается приказом Генерального директора Компании по представлению директоров департаментов. Со всеми изменениями и дополнениями, внесёнными в Перечень, в обязательном порядке должны быть ознакомлены работники Компании.

10. Приложения к Положению

Приложение № 1 – Перечень сведений конфиденциального характера Компании.

Приложение 1
к Положению о сведениях конфиденциального характера
Компании

Перечень сведений конфиденциального характера Компании

№ п/п	Сведения, отнесенные к конфиденциальной информации
I. Сведения об управленческой деятельности Компании	
1.	Отдельные материалы заседаний руководства Компании, совета акционеров и сведения, содержащиеся в них, ограничение доступа к которым установлено решением заседания ПДТК Компании
2.	Сведения (информация), подготовленные Компанией на поступающие из органов государственной власти, предприятий, учреждений и организаций, независимо от организационно-правовой формы и формы собственности с пометкой «Для служебного пользования», «Коммерческая тайна», «Конфиденциально» и другие в части, не содержащей сведений, составляющих государственную тайну
3.	Сведения (информация) о государственном оборонном заказе, не содержащие в своем составе сведений, составляющих государственную тайну
4.	Сведения, содержащиеся в материалах служебной проверки (расследования), до утверждения акта (заключения) по проверке, а также если сведения, полученные в результате проверки (расследования), могут быть использованы в дальнейшем для противоправного действия (нанесения ущерба)
5.	Сведения об организации работы, о конкретных мерах или проводимых мероприятиях, направленных на обеспечение информационной безопасности при осуществлении международного сотрудничества с участием представителей Компании, а также содержащиеся в подготовительных или отчетных документах (формах) о проведении встречи
II. Сведения об административно-хозяйственной деятельности	
6.	Сведения о персональных данных работника Компании, содержащиеся в личном деле работника, кроме случаев, предусмотренных законодательством Российской Федерации
7.	Сведения, получаемые при приеме гражданина на работу в Компанию, необходимые для оформления допуска к государственной тайне
8.	Сведения об осведомленности работника со сведениями, составляющими государственную тайну
9.	Акты проверок деятельности управлений и подведомственных организаций
10.	Сведения о штатном расписании Компании (за исключением общедоступной информации), а также о размерах установленных заработных плат

11.	Сведения о планируемых кадровых решениях в Компании.
III. Сведения о физической и транспортной безопасности	
12.	Система обеспечения пропускного режима принятая в Компании
13.	Акты проверок обеспечения пропускного режима в административное здание Компании
14.	Сведения о результатах оценки уязвимости объектов инфраструктуры Компании
15.	Сведения, содержащиеся в планах обеспечения безопасности перевозок грузов и транспортных средств
IV. Сведения о защите информации	
16.	Сведения об организации обработки информации на средствах вычислительной техники Компании
17.	Сведения, раскрывающие организацию, состояние защиты информации, или носителей информации, или информационного процесса
18.	Сведения о результатах оценки уязвимости информационных систем Компании
19.	Сведения о методах, средствах или эффективности (состоянии защиты) конфиденциальной информации в автоматизированных информационных системах, средствах вычислительной техники, других технических средствах
20.	Обобщенные сведения, содержащиеся в схемах локально–вычислительной сети Компании, с указанием организационно-технологических параметров или технических характеристик и мест расположения ее ответственных составных частей, информационных узлов, которые могут быть определены или определяются на схеме
21.	Сведения о конкретных проводимых и (или) планируемых мероприятиях по информационной безопасности конфиденциальной информации
22.	Сведения о применяемых в Компании программных, программно-аппаратных и иных средствах защиты информации
V. Прочие сведения	
23.	Сведения об организации, состоянии или расположении инженерных систем видеонаблюдения, пожарной или охранной сигнализации здания Компании
24.	Сведения, раскрывающие содержание планов и конкретных мероприятий по охране здания Компании, помещений, в которых выполняются работы, хранятся материалы, ведутся переговоры конфиденциального характера
25.	Данные системы охраны помещений, системы контроля и управления доступом, охранного видеонаблюдения, фиксации системы, электронной системы прохода в помещения Компании