УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ДИРЕКТОРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2018 год

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. ДОЛЖНОСТЬ РАБОТНИКА	Должность относится к категории руководителей. Назначение на должность и освобождение от нее осуществляется приказом Генерального директора ООО «Сатурн»
1.2. СТРУКТУРНОЕ ПОДРАЗДЕЛЕНИЕ	Департамент по безопасности
1.3. ДОЛЖНОСТЬ РУКОВОДИТЕЛЯ	Директор по информационной безопасности находится в подчинении у ____
1.4. КЕМ ЗАМЕЩАЕТСЯ	Ведущий специалист по информационной безопасности
1.5. КОГО ЗАМЕЩАЕТ	___
1.6. РУКОВОДСТВУЕТСЯ	Действующим трудовым законодательством и иными нормативными актами Российской Федерации, внутренними нормативными актами Компании, а также настоящей должностной инструкцией.
1.7. КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ	
1.7.1. Высшее образование в сфере обеспечения безопасности, информационных технологий, защиты информации.	
1.7.2. Опыт работы в бизнес-структурах на руководящих должностях, связанных с обеспечением информационной безопасности от 3 лет.	
1.7.3. Знание принципов организации обеспечения безопасности объектов предприятия, его персонала и информации, являющейся коммерческой тайной и информации относящейся к персональным данным; тактики защиты объектов, информации, персонала предприятия от преступных посягательств.	
1.7.4. Личностные качества: ответственность, коммуникабельность	
1.7.5. Наличие развитых аналитических способностей.	
1.7.6. **Желательно:** Опыт работы в _____ от 5 лет.	

2 ОСНОВНАЯ ЗАДАЧА

2.1. Обеспечение информационной безопасности Компании.
2.2. Организация и проведение мероприятий по защите конфиденциальной информации.
2.3. Мониторинг состояния безопасности Компании с целью выявления рисков, угроз и негативных тенденций на ранних стадиях.

3 ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

3.1 Функциональные обязанности:

3.1.1 Разрабатывать функциональные стратегии, функциональных планов в области обеспечения информационной безопасности.
3.1.2 Планировать выполнение краткосрочных и долгосрочных мероприятий по обеспечению информационной безопасности.
3.1.3 Организовывать планирование и отчетную деятельность в интересах обеспечения информационной безопасности Компании, согласовывать планы работы подразделений информационной безопасности Компании, осуществлять контроль их подготовки и выполнения.
3.1.4 Контролировать полноту и своевременность выполнения функциональных планов, поручений руководства, требований нормативных документов.
3.1.5 Подготавливать предложения по формированию бюджетов и смет затрат, необходимых для решения задач обеспечения информационной безопасности Компании.
3.1.6 Проводить работы по разработке и реализация политики обеспечения информационной безопасности Компании.

3.1.7 Организовывать бесперебойное функционирование систем, обеспечивающих информационную безопасность Компании.
3.1.8 Обеспечивать деятельность по предупреждению нарушений информационной безопасности Компании.
3.1.9 Организовывать мониторинг уязвимостей информационно-телекоммуникационной инфраструктуры Компании
3.1.10 Организовывать работы по профилактике и контролю инцидентов информационной безопасности в Компании (в том числе предупреждать незаконный доступ к информационным ресурсам и утечки конфиденциальной информации).
3.1.11 Организовывать мониторинг действий сотрудников Компании в целях выявления, предупреждения и пресечения нарушений в отношении информационных ресурсов Компании.
3.1.12 Организовывать работы по выявлению факторов и устранению предпосылок к неправомерному использованию инсайдерской информации или информации конфиденциального характера.
3.1.13 Организовывать работы по выработке единых требований (целей, задач, методов и средств работы) по обеспечению информационной безопасности Компании.
3.1.14 Планировать и организовывать работы по развитию и совершенствованию систем, обеспечивающих информационную безопасность.
3.1.15 Организовывать проведение расследований инцидентов безопасности и нарушений в работе информационных систем и сетей Компании, вырабатывать меры по исключению их повторения.
3.1.16 Организовывать проведение служебных расследований по возможным нарушениям сотрудниками Компании требований действующего законодательства и нормативных правовых документов Компании, в результате которых причинен или мог быть причинен информационный ущерб.
3.1.17 Руководить процессом подготовки нормативных правовых документов по линии обеспечения информационной безопасности в Компании, заключений и предложений по проектам локальных нормативных актов Компании.
3.1.18 Организовывать работы по совершенствованию режима защиты коммерческой тайны в области обеспечения соблюдения режима коммерческой тайны (КТ) Компании, в том числе организовывать следующие работы и мероприятия:

- планирование и организация контроля соблюдения режима коммерческой тайны в Компании;
- участие в работе комиссии по пересмотру Перечня информации, составляющей коммерческую тайну;
- разработка требований для Компании по реализации мер соблюдения режима «коммерческая тайна» (далее – КТ);
- разработка нормативных правовых документов и методических рекомендаций в сфере соблюдения режима КТ Компании;
- контроль выполнения требований по реализации мер соблюдения режима КТ Компании;
- проведение расследований по фактам нарушений режима КТ Компании;
- консультирование подразделений и сотрудников Компании по вопросам соблюдения режима КТ;
- информирование руководства Компании о состоянии режима КТ Компании, нарушениях режима КТ, результатах соответствующих проверок и расследований;
- подготовка предложений по совершенствованию режима КТ Компании;
- подготовка предложений по формированию сметы затрат, необходимых для решения задач обеспечения режима КТ.

3.1.19 Организовывать работу в области защиты персональных данных (ПДн) Компании, в том числе организовывать следующие работы и мероприятия:

- разработка требований для подразделений Компании по выполнению законодательства РФ в области защиты ПДн;
- контроль выполнения требований по защите ПДн в Компании;
- разработка нормативно-методических документов в сфере защиты ПДн в Компании;

- проведение расследований по фактам нарушения норм защиты ПДн в Компании;
- консультирование подразделений и сотрудников Компании по вопросам защиты ПДн;
- информирование Руководства о состоянии защиты ПДн в Компании, о нарушениях норм защиты ПДн, о результатах соответствующих проверок и расследований;
- разработка предложений по совершенствованию защиты ПДн Компании;
- разработка предложений по формированию сметы затрат, необходимых для решения задач обеспечения защиты ПДн в Компании.

3.1.20 Организовывать процесс обеспечения защиты персональных данных Компании.
3.1.21 Руководить работами по разработке моделей угроз и нарушителя персональных данных.
3.1.22 Участвовать в процессе категорирования информационных систем персональных данных Компании.
3.1.23 Подготавливать предложения руководству Компании и Совету директоров по реализации мер, направленных на достижение поставленных целей и задач в области обеспечения информационной безопасности.
3.1.24 Обеспечивать контроль за соблюдением выполнения правил обработки персональных данных.
3.1.25 Взаимодействовать с регулирующими органами Российской федерации по вопросам обеспечения защиты персональных данных.
3.1.26 Организовывать мероприятия по лицензированию деятельности Компании в области технической защиты конфиденциальной информации.
3.1.27 Организовывать взаимодействие между структурными подразделениями Компании для достижения целей обеспечения требуемого уровня информационной безопасности.
3.1.28 Осуществлять методическую помощь подразделениям информационной безопасности Компании при подготовке распорядительных и нормативных документов по линии обеспечения информационной безопасности.
3.1.29 Участвовать в создании и внедрении единых форм и методов в деятельности подразделений безопасности Компании.
3.1.30 Получать, обобщать и анализировать результаты, принимаемые в Компании меры в области информационной безопасности, прогнозировать развитие событий в информационной сфере, подготавливать заключения и рекомендации.
3.1.31 Организовывать и проводить совещания с руководством подразделений безопасности Компании по вопросам совершенствования работы в сфере обеспечения информационной безопасности.
3.1.32 Организовывать и контролировать деятельности ПБ Компании в области информационной безопасности.
3.1.33 Реализовывать процесс управления рисками информационной безопасности и выработке мер по их минимизации.
3.1.34 Организовывать работы по выявлению бизнес-процессов Компании, в ходе которых возникают угрозы информационным ресурсам и требующие принятия дополнительных мер по обеспечению информационной безопасности.
3.1.35 Подготавливать информацию для руководства Компании об угрозах информационной безопасности Компании, действиях работников Компании, которые могут нанести или наносят материальный ущерб или ущерб деловой репутации (имиджу) Компании, проблемах обеспечения защиты конфиденциальной информации, нарушениях функционирования информационно-телекоммуникационной инфраструктуры, для выработки оптимальных управленческих решений.
3.1.36 Руководить работами по оценке уровня зрелости Компании в области обеспечения и управления информационной безопасностью.
3.1.37 Организовывать работы по повышению осведомленности сотрудников Компании в вопросах обеспечения информационной безопасности.
3.1.38 Организовывать проведение проверочных мероприятий в области обеспечения защиты конфиденциальной информации в структурных подразделениях Компании.
3.1.39 Организовывать работы по сопровождению деятельности Компании в сфере информационных технологий, участию в проектах по внедрению информационных систем в

части контроля соответствия требованиям нормативных правовых документов РФ и Компании по вопросам обеспечения информационной безопасности.

3.1.40 Анализировать работы подчиненных и определять степень соответствия их профессиональных возможностей поставленным перед ними целям и задачам.

3.1.41 Оценивать качество работы, выполняемой подчиненными в соответствии с действующими в Компании нормативными документами.

3.1.42 Разрабатывать должностные инструкции работников подразделения.

3.1.43 Участвовать в подборе новых работников на вакантные должности.

3.1.44 При выполнении трудовых обязанностей руководствоваться законодательством и нормативными актами РФ, внутренними нормативными документами Компании, трудовым договором, а также настоящей должностной инструкцией, исполнять поручения, распоряжения и рекомендации органов управления и комитетов Компании, а также своего непосредственного и вышестоящего Руководителей.

3.1.45 Знать и соблюдать требования, правила и ограничения, установленные Правилами внутреннего трудового распорядка и иными внутренними нормативными документами Компании, в т. ч. в области трудовой дисциплины, управления рисками, предотвращения коррупции, соблюдения деловой и профессиональной этики, пожарной безопасности и других областях.

3.1.46 Знать и соблюдать требования внутренних нормативных документов Компании, определяющих правила, требования и ограничения по работе с конфиденциальной информацией и ее охране, в том числе не использовать, не раскрывать, не разглашать, не передавать и не комментировать конфиденциальную информацию о Компании,), его сотрудниках, контрагентах и иных лицах, иначе как в рамках добросовестного и надлежащего исполнения своих должностных обязанностей в Компании.

3.1.47 Знать (а) Перечень информации, составляющей коммерческую тайну Компании («ИКТ»), порядок его формирования и изменения, (б) Методику классификации ИКТ Компании в зависимости от ее коммерческой ценности и размера ущерба, наносимого при ее несанкционированном разглашении, передаче и/или доступе к ней, (в) Перечень информации, относящейся к инсайдерской информации Компании уметь применять указанные документы на практике, в том числе, своевременно идентифицировать описанные в них типы информации.

3.1.48 Контролировать подготовку, заключение и исполнение договоров/сделок, по которым Работник является ответственным исполнителем, для идентификации инсайдерской информации Компании, передаваемой контрагентам, в т. ч. при переговорах и обмене корреспонденцией, при этом Работник обязан незамедлительно оповещать Заместителя Генерального директора по безопасности и ИТ, что:

(а) договоры с контрагентами или сопутствующая документация (включая переписку) на стадии согласования, подписания или передачи контрагентам содержат инсайдерскую информацию Компании;

(б) контрагентам передается инсайдерская информация Компании или предоставляется доступ к ней в ходе исполнения заключенных договоров/сделок в тех случаях, когда на стадии согласования/подписания договорной документации контрагентам не передавалась инсайдерская информация и/или они не имели доступа к ней;

(в) переданная контрагентам инсайдерская информация Компании перестала считаться инсайдерской, в т. ч., в силу ее надлежащего публичного раскрытия, утраты актуальности или по иным причинам;

(г) доступ контрагента(-ов) к инсайдерской информации был прекращен.

3.1.49 Обеспечивать контроль исполнения условий договоров с целью исключения причин образования просроченной дебиторской задолженности.

3.1.50 По мере поступления в подразделение Руководителя управления делами получать там конфиденциальные документы (КД) и немедленно регистрировать установленным порядком в Журнале учета документов.

3.1.51 Передавать документы для исполнения работникам подразделения только в соответствии с резолюциями на них (указаниями по ознакомлению) под роспись работников в Журнале учета.

3.1.52 Знать Номенклатуру должностей работников Компании, которым необходим допуск к информации, составляющей коммерческую тайну в части допущенных к ИКТ работников своего структурного подразделения, не допускать ознакомление с КД работников, должности которых не включены в Номенклатуру и не подписавших трудовой договор (дополнительное соглашение к нему), регулирующие отношения работника и Компании по использованию ИКТ, а также работников, которым КД не адресован для исполнения.
3.1.53 Готовить по указанию Руководителя структурного подразделения служебные записки по внесению изменений в Перечень информации, составляющей коммерческую тайну Компании, оказывать помощь работникам подразделения по отнесению той или иной информации к ИКТ и нанесению на них грифа «Коммерческая тайна» и иных необходимых реквизитов.
3.1.54 Знать Методику классификации ИКТ Компании в зависимости от ее коммерческой ценности и размера ущерба, наносимого при ее разглашении и/или неправомерном доступе к ней, уметь применять ее на практике. Оказывать помощь работникам подразделения в определении уровня классификации конкретных КД.
3.1.55 Готовить по указанию Руководителя структурного подразделения служебные записки о снятии ограничений на доступ к ИКТ в связи с потерей ей актуальности или необходимостью раскрытия в соответствии с требованиями законодательства и регуляторов, о пересмотре уровня конфиденциальности КД.
3.1.56 Периодически, но не реже одного раза в неделю, проводить проверки служебных помещений структурного подразделения на предмет соблюдения порядка хранения и уничтожения КД, их проектов и черновиков, выполнения требований режима коммерческой тайны, установленных Кодексом «Безопасность». О выявленных недостатках сообщать служебной запиской Руководителю структурного подразделения, по его указанию готовить соответствию информацию для Заместителя Генерального директора по безопасности и ИТ.
3.1.57 Периодически, но не реже одного раза в месяц, проводить проверку наличия КД у исполнителей, о результатах проверки служебной запиской сообщать Руководителю подразделения.
3.1.58 Участвовать в работе комиссий по ежегодной проверке наличия КД, отбору и уничтожению не требующихся для дальнейшего использования и потерявших актуальность материальных носителей ИКТ.

3.1.59 Анализировать работу подчиненных и определять степень соответствия их профессиональных возможностей поставленным перед ними целям и задачам.
3.1.60 Оценивать качество работы, выполняемой подчиненными в соответствии с действующими в Компании нормативными документами.
3.1.61 Разрабатывать должностные инструкции на должности, находящиеся в подчинении.
3.1.62 Способствовать развитию и повышению квалификации подчиненных Работников.
3.1.63 Участвовать в подборе новых Работников на вакантные должности.
3.1.64 Проводить инструктаж подчиненных по вопросам деятельности подразделения и Компании.
3.1.65 Осуществлять взаимодействие своего подразделения с другими подразделениями Компании.
3.1.66 Составлять графики отпусков Работников своего подразделения.
3.1.67 Осуществлять контроль соблюдения режима рабочего времени подчиненными работниками и обеспечивать учет рабочего времени в соответствии с законодательством и нормативными документами Компании.
3.1.68 Проводить периодические инструктажи на рабочем месте по правилам охраны труда, техники безопасности, производственной санитарии.

4 ИМЕЕТ ПРАВО

4.1. Запрашивать документы, материалы и другую информацию, необходимую для исполнения должностных обязанностей.
4.2. Принимать участие в обсуждении вопросов, касающихся деятельности своего структурного подразделения.
4.3. Участвовать в мероприятиях Компании в рамках своей компетенции.
4.4. Вести деловую переписку и представлять интересы Компании в пределах своей компетенции.
4.5. Подписывать и визировать документы, в пределах своей компетенции (для лиц, имеющих право подписывать и визировать документы).
4.6. Вносить предложения по оптимизации работы своего структурного подразделения и всей Компании.
4.7. Быть обеспеченным необходимыми техническими и программными средствами для выполнения в срок поставленных задач.

5 НЕСЕТ ОТВЕТСТВЕННОСТЬ

5.1 За невыполнение указаний и поручений руководства Компании, указаний непосредственного Руководителя, плана работ и несоблюдение условий труда Работников, находящихся в подчинении.

5.2 За нечеткое и несвоевременное выполнение своих должностных обязанностей, предусмотренных настоящей инструкцией.

5.3 За сохранность находящегося в использовании имущества.

5.4 За несоблюдение трудовой дисциплины, Правил внутреннего трудового распорядка, иных локальных нормативных актов Компании.

5.5 За ненадлежащее или несанкционированное использование, раскрытие, разглашение, распространение, передачу или комментирование конфиденциальной информации (включая ИКТ и инсайдерскую информацию) о Компании, его сотрудниках или контрагентах (в т. ч. за совершение сделок с ценными бумагами на основании такой информации), утрату документов, содержащих такую информацию, нарушение установленных правил обращения с ней, сбор сведений, составляющих конфиденциальную информацию, если это не является необходимым для надлежащего осуществления своих должностных обязанностей, незаконное получение денег, ценных бумаг, услуг, иного имущества, а равно незаконное пользование услугами имущественного характера, за совершение неправомерных или неэтичных действий (бездействия) в связи с занимаемым служебным положением, неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для персональных компьютеров, нарушение правил эксплуатации персональных компьютеров или их сети и другие типы нарушений.

РЕКВИЗИТЫ СТОРОН

РАЗРАБОТАЛ:			
	Директор по информационной безопасности	_____ (подпись)	
СОГЛАСОВАНО:			
	Заместитель Генерального директора по безопасности	_____ (подпись)	
		_____ (подпись)	

ЛИСТ ОЗНАКОМЛЕНИЯ

С должностной инструкцией ознакомлен(а) и обязуюсь выполнять свои обязанности согласно должностной инструкции. Один экземпляр должностной инструкции мною получен:

№ п/п	ФИО	Подпись	Дата