|  |  |
| --- | --- |
| СОГЛАСОВАНО Протокол заседания профсоюзного комитета  ООО «Солнышко»  от «\_17\_» \_октября\_20\_22\_\_г. | УТВЕРЖДАЮ  Генеральный директор  ООО «Солнышко»  Иванов /\_В.С. Иванов\_  «\_17\_» \_октября\_20\_22\_\_г. |
|  |  |

**Положение об отделе защиты информации**

**ООО «Солнышко»**

**I. Общие положения**

1. Настоящее положение определяет цели, задачи и функции Отдела защиты информации ООО «Солнышко», обеспечивающего информационную безопасность организации (далее - подразделение).

2. Подразделение в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, другими нормативными правовыми документами в сфере обеспечения информационной безопасности, указаниями руководителя ООО Солнышко (далее - организация) и настоящим положением.

3. Подразделение подчинено заместителю руководителя организации, ответственному за обеспечение информационной безопасности в организации, либо иным лицам из состава руководства организации при условии осуществления курирования со стороны руководителя организации.

4. Контроль за деятельностью подразделения осуществляет руководитель организации.

**II. Цели и задачи деятельности подразделения**

5. Деятельность подразделения направлена:

а) на исключение или существенное снижение негативных последствий (ущерба) в отношении организации вследствие нарушения функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления в результате реализации угроз безопасности информации;

б) на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

в) на повышение защищенности организации от возможного нанесения ему (ей) материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем организации или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования;

г) на обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры организации;

д) на обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем и информационно-телекоммуникационной инфраструктуры организации.

6. Основными задачами деятельности подразделения являются:

а) планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в организации;

б) выявление угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств;

в) предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

г) поддержание стабильной деятельности организации и ее производственных процессов в случае проведения компьютерных атак;

д) взаимодействие с Национальным координационным центром по компьютерным инцидентам;

е) обеспечение нормативно-правового обеспечения использования информационных ресурсов.

**III. Функции подразделения**

 7. Подразделение выполняет следующие функции:

а) разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в организации и подведомственных организациях;

б) разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в организации и представление их руководителю организации;

в) выявление и проведение анализа угроз безопасности информации в отношении организации, уязвимостей информационных систем, программного обеспечения программно-аппаратных средств и принятие мер по их устранению;

г) обеспечение в соответствии с требованиями по информационной безопасности, в том числе с целью исключения (невозможности реализации) негативных последствий, разработки и реализации организационных мер и применения средств обеспечения информационной безопасности;

д) обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;

е) представление в Национальный координационный центр по компьютерным инцидентам информации о выявленных компьютерных инцидентах;

ж) исполнение указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами, Федеральной службой по техническому и экспортному контролю по результатам мониторинга защищенности информационных ресурсов, принадлежащих организации либо используемых организацией, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети "Интернет";

з) проведение анализа и контроля за состоянием защищенности систем и сетей и разработка предложений по модернизации (трансформации) основных процессов организации в целях обеспечения информационной безопасности в организации;

и) подготовка отчетов о состоянии работ по обеспечению информационной безопасности в организации;

к) организация развития навыков безопасного поведения в организации, в том числе проведение занятий с руководящим составом и специалистами организации по вопросам обеспечения информационной безопасности;

л) выполнение иных функций, исходя из поставленных руководством организации целей и задач в рамках обеспечения информационной безопасности в организации, подведомственных организациях.

**IV. Права подразделения**

8. С целью реализации функций подразделение имеет право:

а) запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений организации, необходимым для принятия решений по всем вопросам, отнесенным к компетенции подразделения;

б) готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности организаций, имеющих лицензии на соответствующий вид деятельности;

в) контролировать деятельность любого структурного подразделения организации по выполнению требований к обеспечению информационной безопасности;

г) постоянно повышать профессиональные компетенции, знания и навыки работников в области обеспечения информационной безопасности;

д) участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;

е) участвовать в работе комиссий организации при рассмотрении вопросов обеспечения информационной безопасности;

ж) вносить предложения руководству организации о приостановлении работ в случае обнаружения факта нарушения информационной безопасности;

з) вносить представления руководству организации в отношении государственных служащих, муниципальных служащих и работников организации (далее - работники) при обнаружении фактов нарушения работниками установленных требований безопасности информации в организации, в том числе ходатайствовать о привлечении указанных работников к административной или уголовной ответственности;

и) вносить на рассмотрение руководству организации предложения по вопросам деятельности подразделения.

**V. Взаимоотношения и связи подразделения**

9. Подразделение осуществляет свои полномочия во взаимодействии со структурными подразделениями организации и подведомственными ему организациями, а также в пределах своей компетенции с иными организациями и гражданами в установленном порядке.

10. По указанию руководства осуществляет взаимодействие с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации по вопросам информационной безопасности.

**VI. Показатели эффективности и результативности подразделения**

11. Эффективность и результативность деятельности подразделения определяются по итогам выполнения организацией, а также подведомственными ему организациями программы обеспечения информационной безопасности с учетом приоритетных целей, предусмотренных разделом II настоящего типового положения.

12. Работники подразделения несут ответственность за выполнение возложенных на них обязанностей в соответствии с должностными регламентами, утверждаемыми руководителем организации либо должностным лицом, наделенным руководителем организации соответствующими полномочиями.