|  |  |
| --- | --- |
| ООО «InfoSecure» | Утверждаю  Генеральный директор  Узумаки Н.М. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  от 04.09.2023  Юридический адрес: 123456, г. Москва, ул. Примерная, д. 1, офис 101 |

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

Специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры

1. Общие положения

1.1. Настоящая должностная инструкция определяет и регламентирует полномочия, функциональные и должностные обязанности, права и ответственность специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры InfoSecure.

1.2. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры относится к категории специалистов, назначается на должность и освобождается от должности в установленном действующим трудовым законодательством порядке приказом руководителя Компании.

1.3. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры подчиняется непосредственно директору InfoSecure.

1.4. На должность специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры назначается лицо, имеющее высшее профессиональное образование по специальности «Информационная безопасность» без предъявления требований к стажу работы.

1.5. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры должен знать:

* законы и иные нормативные правовые акты Российской Федерации, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа;
* нормативные и методические документы по вопросам, связанным с обеспечением безопасности информации;
* структуру управления, связи и автоматизации и основные элементы ключевой системы информационной инфраструктуры организации;
* подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты от преднамеренных воздействий, контроля целостности информации;
* порядок создания защищенного канала между взаимодействующими объектами через систему общего пользования с использованием выделенных каналов связи;
* порядок осуществления аутентификации взаимодействующих объектов и проверки подлинности отправителя и целостности, передаваемых через систему общего пользования данных;
* оснащенность организации основными и вспомогательными техническими средствами и системами, перспективы их развития и модернизации;
* перспективы и направления развития методов и средств технических и программно-аппаратных средств защиты информации от деструктивных информационных воздействий;
* порядок проектирования и аттестации объектов информатизации;
* контроль эффективности защиты информации на объектах информатизации;
* порядок осуществления контроля использования открытых каналов радиосвязи;
* методы и средства выявления угроз безопасности информации, методики выявления каналов утечки информации;
* методы проведения научных исследований, разработок по технической защите информации;
* порядок обследования ключевых систем информационной инфраструктуры, составления актов проверки, протоколов испытаний, предписаний на право эксплуатации специальных средств обеспечения безопасности информации, а также положений, инструкций и других организационно-распорядительных документов;
* полномочия по вопросам обеспечения безопасности информации, возможности и порядок применения штатных технических средств обеспечения безопасности информации и контроля их эффективности;
* методы анализа результатов проверок, учета нарушений требований по обеспечению безопасности информации;
* методику подготовки предложений, методы и средства выполнения вычислительных работ в интересах планирования, организации и проведения работ по обеспечению безопасности информации и обеспечению государственной тайны;
* достижения науки и техники в стране и за рубежом в области технической разведки и защиты информации;
* методы оценки профессионального уровня специалистов по обеспечению безопасности информации, аттестации специалистов;
* основы трудового законодательства;
* правила по охране труда и пожарной безопасности.

1.6. Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры в своей деятельности руководствуется:

* требованиями законодательства РФ;
* локальными актами и организационно-распорядительными документами Компании;
* правилами внутреннего трудового распорядка;
* правилами охраны труда и техники безопасности, обеспечения производственной санитарии и противопожарной защиты;
* указаниями, приказаниями, решениями и поручениями непосредственного руководителя;
* настоящей должностной инструкцией.

1.7. В период временного отсутствия специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (отпуск, болезнь, прочее), его обязанности возлагаются на старшего специалиста по защите информации ,который назначается в установленном порядке, приобретает соответствующие права и несет ответственность за неисполнение или ненадлежащее исполнение обязанностей, возложенных на него в связи с замещением.

2. Должностные обязанности

Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры выполняет следующие должностные обязанности:

2.1. Выполняет мероприятия по обеспечению безопасности информации в ключевых системах информационной инфраструктуры.

2.2. Определяет возможные угрозы безопасности информации, уязвимость программного и аппаратного обеспечения, разрабатывает технологии обнаружения вторжения, оценивает и переоценивает риски, связанные с угрозами деструктивных информационных воздействий, способных нанести ущерб системам и сетям вследствие несанкционированного доступа, использования раскрытия, модификации или уничтожения информации и ресурсов информационно-управляющих систем.

2.3. Определяет ограничения по вводу информации, процедуры управления инцидентами нарушения безопасности и предотвращает их развитие, порядок подключения к открытым информационным системам с учетом обеспечения безопасности, связанной с соглашениями о доступе и приоритезации ресурсов, требования к местам резервного хранения, обработки и копирования информации, приоритеты обслуживания по использованию основных и резервных телекоммуникационных сервисов (услуг).

2.4. Разрабатывает процедуры защиты носителей информации, коммуникаций и восстановления информационно-управляющих систем после сбоя или отказа.

2.5. Осуществляет контроль деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры; информационное, материально-техническое и научно-техническое обеспечение безопасности информации; контроль состояния работ по обеспечению безопасности информации в ключевых системах информационной инфраструктуры и их соответствие нормативным правовым актам Российской Федерации.

2.6. Дает отзывы и заключения на проекты вновь создаваемых и модернизируемых объектов и других разработок по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры.

2.7. Участвует в рассмотрении технических заданий на научно-исследовательские и опытно-конструкторские работы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, оценивает их соответствие действующим нормативным и методическим документам.

2.8. Участвует в работах по внедрению новых средств технической защиты информации.

2.9. Содействует распространению в организации передового опыта и внедрению современных организационно-технических мер, средств и способов обеспечения безопасности информации в ключевых системах информационной инфраструктуры.

2.10. Проводит оценки технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры.

2.11. Разрабатывает списки доступа персонала на объекты защиты, порядок и правила поведения работников, в том числе при их перемещении, увольнении и взаимодействии с персоналом сторонних организаций.

2.12. Осуществляет руководство и обучение персонала действиям в кризисных ситуациях, включая порядок действий руководящих и других ответственных лиц ключевых систем информационной инфраструктуры.

В случае служебной необходимости специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры может привлекаться к выполнению своих должностных обязанностей сверхурочно, по решению заместителя директора по производству, в порядке, предусмотренном законодательством.

3. Права

Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры имеет право:

3.1. Знакомиться с проектами решений руководства Компании, касающимися его деятельности.

3.2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями

3.3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех выявленных в процессе своей деятельности недостатках и вносить предложения по их устранению.

3.4. Запрашивать лично или по поручению руководства Компании от подразделений организации и иных специалистов информацию и документы, необходимые для выполнения своих должностных обязанностей.

3.5. Привлекать специалистов всех (отдельных) структурных подразделений к решению возложенных на него задач.

3.6. Требовать от руководства организации оказания содействия в исполнении своих должностных обязанностей.

4. Ответственность

Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры несет административную, дисциплинарную и материальную (а в отдельных случаях, предусмотренных законодательством РФ, — и уголовную) ответственность за:

4.1. Невыполнение или ненадлежащее выполнение служебных указаний непосредственного руководителя.

4.2. Невыполнение или ненадлежащее выполнение своих трудовых функций и порученных ему задач.

4.3. Неправомерное использование предоставленных служебных полномочий, а также использование их в личных целях.

4.4. Недостоверную информацию о состоянии выполнения порученной ему работы.

4.5. Непринятие мер по пресечению выявленных нарушений правил техники безопасности, противопожарных и других правил, создающих угрозу деятельности предприятия и его работникам.

4.6. Не обеспечение соблюдения трудовой дисциплины.

5. Условия работы

5.1. Режим работы специалиста по обеспечению безопасности информации в ключевых системах информационной инфраструктуры определяется в соответствии с правилами внутреннего трудового распорядка, установленными в Компании.

5.2. В связи с производственной необходимостью специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры обязан выезжать в служебные командировки (в том числе местного значения).

С инструкцией ознакомлен \_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/ «\_\_» \_\_\_\_\_\_\_ 20\_\_ г.

(подпись)