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

**Положение об отделе по защите информации**

1. **Общие положения**
   1. Отдел защиты информации является структурным подразделением Службы безопасности в организации InfoSecure.
   2. Деятельность Отдела регулируется действующим законодательством, Уставом организации InfoSecure, Положением о Службе безопасности организации, а также настоящим Положением.
   3. Отдел защиты информации организует и координирует деятельность всех подразделений InfoSecure по комплексной защите информации, контролю и оценке эффективности мер, направленных на обеспечение информационной безопасности в организации InfoSecure.
   4. Отдел защиты информации возглавляется начальником отдела. Начальник отдела назначается на должность и освобождается от занимаемой должности в установленном порядке по представлению начальника Службы Безопасности InfoSecure.
   5. Структура и штатное расписание отдела определяются в установленном порядке, в соответствии с объемами работ, задачами и функциями, исполняемыми отделом.
2. **Основные задачи и функции отдела**
   1. Основными задачами отдела защиты информации являются:
3. разработка единой политики (концепции) обеспечения информационной безопасности INFOSECURE, определение требований к системе защиты информации INFOSECURE и документообороту на бумажных и электронных носителях;
4. организация мероприятий и координация работ всех подразделений INFOSECURE по комплексной защите информации на всех этапах технологических циклов ее создания, переноса на носитель (бумажный или электронный), обработки и передачи в соответствии с единой политикой обеспечения информационной безопасности INFOSECURE;
5. контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

Основными функциями отдела защиты информации являются:

1. организация и координация действий подразделений INFOSECURE по вопросам обеспечения информационной безопасности;
2. экспертиза договоров INFOSECURE со сторонними организациями по вопросам ОБИ при передаче (приеме) информации;
3. участие в работе технической комиссии по пересмотру Перечня сведений, подлежащих защите
4. согласование технических порядков по технологиям, связанным с информационным обменом и документооборотом;
5. участие в проектировании, приемке, сдаче в промышленную эксплуатацию программных средств и АС INFOSECURE (в части требований к средствам защиты информации);
6. контроль за соблюдением правил безопасной эксплуатации АС INFOSECURE;
7. контроль за соблюдением требований ТУ и сертификатов на приобретенные программные и аппаратные средства (в том числе средства защиты информации);
8. организация и контроль за разрешительной системой допуска исполнителей к работе с защищаемой информацией;
9. определение порядка учета, хранения и обращения с защищаемой информацией (документами и носителями информации);
10. контроль за сохранностью конфиденциальных документов и носителей информации;
11. генерация ключей шифрования и ЭЦП.
12. **Руководство. Права и обязанности, ответственность**
    1. Для решения задач, возложенных на отдел защиты информации, сотрудники этого отдела должны иметь следующие права:
13. определять необходимость и разрабатывать нормативные документы, касающиеся вопросов ОБИ, включая документы, регламентирующие деятельность сотрудников подразделений INFOSECURE;
14. получать информацию от сотрудников подразделений INFOSECURE по вопросам применения технологий обработки информации и эксплуатации АС;
15. участвовать в проработке технических решений по вопросам ОБИ при проектировании и разработке комплексов задач (задач);
16. участвовать в испытаниях разработанных комплексов задач (задач) по вопросам оценки качества реализации требований по ОБИ;
17. контролировать деятельность сотрудников подразделений INFOSECURE по вопросам ОБИ.
    1. Начальник отдела защиты информации осуществляет в полной мере руководство деятельностью отдела, несет ответственность за надлежащее исполнение возложенных на него обязанностей и обеспечивает:
18. исполнение отделом задач и функций, определенных настоящим положением, в соответствии с действующим законодательством и нормативными документами INFOSECURE;
19. обеспечивает соблюдение сотрудниками отдела установленных правил трудового распорядка, производственной и технологической дисциплины;
20. разрабатывает и вносит на рассмотрение начальника Службы безопасности предложения по совершенствованию структуры отдела и повышению уровня подготовки сотрудников отдела, улучшение работы и иные предложения по вопросам, входящим в его компетенцию;
21. организует техническое обучение и повышение квалификации сотрудников отдела;
22. обеспечивает реализацию мероприятий по созданию безопасных условий труда сотрудников отдела на всех технологических участках;
23. обеспечивает контроль за соблюдением сотрудниками отдела правил электро- и пожарной безопасности;
24. распределяет обязанности и разрабатывает должностные инструкции сотрудников отдела;
25. представляет сотрудников отдела для назначения или освобождения от должности, поощрения отличившихся работников, наложения дисциплинарных взысканий в соответствии с действующим законодательством о труде и правилами внутреннего трудового распорядка;
26. разрабатывает, представляет на утверждение и обеспечивает контроль за порядком доступа в служебные помещения отдела;
27. устанавливает регламент проведения профилактических, ремонтных и аварийных работ на установленном в отделе оборудовании;
28. координирует совместную деятельность сотрудников отдела со структурными подразделениями Службы безопасности и другими подразделениями INFOSECURE;
29. участвует в совещаниях по вопросам информационной безопасности INFOSECURE и представляет Службу безопасности INFOSECURE в других учреждениях и организациях по поручению начальника Службы безопасности.
    1. Начальник отдела защиты информации отвечает за организацию мероприятий по выполнению требований обеспечения безопасности информации при работе на АРМ АС INFOSECURE. Он обеспечивает:
30. планирование и организацию практических мероприятий по предотвращению попыток несанкционированного вмешательства в процесс нормального функционирования АС и попыток НСД к обрабатываемой, хранимой и отображаемой на ПЭВМ АС INFOSECURE информации;
31. организацию постоянного контроля за соблюдением сотрудниками INFOSECURE требований Планов защиты конкретных АС и других организационно-распорядительных документов по вопросам обеспечения безопасности информации;
32. определение особых обязанностей должностных лиц INFOSECURE по обеспечению безопасности информации при их работе в АС;
33. организацию проведения занятий с персоналом INFOSECURE по изучению организационно-распорядительных документов по всему комплексу вопросов обеспечения безопасности информации при работе в АС;
34. организацию проведения работ по выявлению возможных каналов нарушения информационной безопасности при эксплуатации АС и принятие своевременных мер по их перекрытию;
35. определение и пересмотр порядка установки и модернизации аппаратных и программных средств АС INFOSECURE в части обеспечения безопасности информации и процессов ее обработки;
36. определение и пересмотр порядка проектирования, разработки, отладки, проверки, внедрения и использования программного обеспечения в части обеспечения безопасности информации и процессов ее обработки.
    1. Сотрудники отдела защиты информации обязаны:
37. проводить практические мероприятия по предотвращению незаконного вмешательства в процесс функционирования системы и несанкционированного доступа (НСД) к информации, обрабатываемой, хранимой и отображаемой на АРМ АС INFOSECURE;
38. периодически контролировать правильность ведения журналов учета нештатных ситуаций и формуляров АРМ в подразделениях INFOSECURE;
39. проводить занятия с сотрудниками подразделений INFOSECURE по правилам работы на ПЭВМ и по изучению руководящих документов по вопросам обеспечения безопасности информации;
40. контролировать выполнение обязанностей администраторами безопасности АС, ответственными за информационную безопасность в подразделениях, ответственными за эксплуатацию конкретных АРМ, за обслуживание определенных технических и программных средств;
41. участвовать в работе по определению необходимых мер защиты при проектировании программных средств автоматизации решения прикладных задач, по оценке качества реализации необходимых защитных механизмов в АС при испытаниях и внедрении данного программного обеспечения (в части обеспечения безопасности информации и процессов ее обработки);
42. контролировать исполнение порядка учета, хранения, использования и уничтожения отчуждаемых магнитных носителей конфиденциальной информации;
43. контролировать выполнение установленных правил создания, хранения и использования эталонных копий программных средств, соблюдение порядка формирования и использования информационных массивов и баз данных, резервного и архивного копирования данных;
44. координировать действия должностных лиц по своевременному восстановлению процесса обработки данных в кризисных (аварийных) ситуациях;
45. участвовать в расследовании причин возникновения серьезных кризисных ситуаций;
46. постоянно проводить работу по выявлению возможных каналов утечки конфиденциальных сведений при эксплуатации АС и несанкционированного вмешательства в процесс ее функционирования, готовить предложения по совершенствованию системы защиты и пересмотру Плана защиты;
47. участвовать в работе комиссий по пересмотру Плана защиты АС.

4.Взаимодействия и связи:

1. СЗИ взаимодействует с государственными учреждениями и организациями в соответствии с запросами и требованиями, предъявляемыми ими в рамках соблюдения законодательства и политики предприятия.

2. Взаимодействие с филиалами:

2.1. Для обеспечения безопасного взаимодействия с филиалами разработаны процедуры обмена информацией между головным офисом и филиалами с учетом безопасности. Подробные методы шифрования и защиты данных описаны в "Процедуры обмена информацией с филиалами".

2.2. Установлены процедуры контроля доступа к информации и ресурсам предприятия среди филиалов. Эти процедуры включают в себя:

* Методы аутентификации сотрудников, подробно описанные в "Процедура аутентификации сотрудников".
* Регулярные проверки прав доступа, проводимые в соответствии с "Процедура проверки прав доступа".
* Уведомление о доступе и его мониторинг, подробности которого описаны в "Процедура мониторинга доступа".

3. Взаимодействие с государственными учреждениями и организациями:

3.1. Для обработки запросов из государственных органов и организаций разработаны процедуры, подробно описанные в "Процедура обработки запросов из государственных органов".

3.2. Определены ответственные лица, уполномоченные на взаимодействие с запросами от государственных органов и организаций. Процедуры уведомления органов о выполнении запросов подробно описаны в "Процедура уведомления государственных органов".

4. Учет и обработка запросов:

4.1. Установлены сроки реагирования на запросы из государственных учреждений и организаций, а также процедуры мониторинга и отслеживания статуса запросов, как описано в "Процедура учета и обработки запросов".

4.2. Разработаны механизмы обеспечения конфиденциальности информации при работе с запросами, включая шифрование данных и ограничение доступа. Подробности механизмов описаны в "Механизмы обеспечения конфиденциальности при работе с запросами".

5.Финансирование работ и материально-техническое обеспечение:

Финансирование деятельности СЗИ осуществляется за счет средств предприятия. Финансирование включает в себя следующие аспекты:

* Разработка бюджета СЗИ на основе потребностей и планов.
* Приобретение и обновление технических средств и программного обеспечения.
* Закупка и обслуживание оборудования для мониторинга и обнаружения инцидентов.
* Оплата обучения сотрудников вопросам информационной безопасности.
* Финансирование профилактических мероприятий и реагирования на инциденты

6.Имущество и средства:

СЗИ имеет доступ к следующему имуществу и средствам:

* Аппаратные средства, программное обеспечение, средства связи и другое оборудование, необходимое для обеспечения информационной безопасности.
* Средства автоматизации, системы мониторинга и обнаружения инцидентов, системы контроля доступа и аутентификации.
* Антивирусные программы, брандмауэры, средства шифрования и другие технические средства защиты.
* Документацию, включая политику информационной безопасности, процедуры, инструкции и другие документы, необходимые для обучения сотрудников и обеспечения безопасности.

7.Трудовые отношения:

Трудовые отношения с сотрудниками СЗИ регулируются трудовым законодательством и локальными нормативными актами предприятия.

|  |  |
| --- | --- |
| **РАЗРАБОТАЛ:**  Начальник СЗИ | \_\_\_\_\_\_\_\_\_\_\_\_\_/С.Ф.Учиха/ |
| **СОГЛАСОВАНО:**  Экономист | \_\_\_\_\_\_\_\_\_\_\_\_\_/С.В.Корнилкин/ |