Политика ИБ

Компания ЗАО «ПАРАВОЗ». Штат — 250 сотрудников, 20 руководство, 30 бухгалтерия, 50 — IT-отдел, 100 — менеджеры по работе с клиентами, 50 — отдел безопасности.

1. Общее положение ЗАО «ПАРАВОЗ»

1.1 Настоящая Политика разработана в соответствии с действующим законодательством, нормативными актами и соотносимыми с ними положениями внутренних документов ЗАО «ПАРАВОЗ» Она регламентирует порядок организации с целью обеспечения сохранности информации и ее безопасности в сфере предоставления коммунальных услуг как в осуществлении текущей деятельности, так и в обозримом будущем.

1.2. Предметом настоящего документа является:

· порядок доступа к конфиденциальной информации;

· физическая безопасность (доступ в помещения);

· работа в глобальной сети Интернет;

2.Порядок доступа к конфиденциальной информации

В целях обеспечения защиты информации в ЗАО «ПАРАВОЗ», устанавливается следующий порядок допуска к работе с конфиденциальными источниками:

А) Право доступа сотрудников к данным пользователей услуг осуществляется только с помощью электронного пропуска полученного от руководства

Б) Конфиденциальная информация о пользователе доступна только руководству и сотрудникам со спец пропуском

В) Информация о задолженностях и об оплаченных услугах пользователя доступна всем сотрудникам организации

Г) Категорически запрещается использование флэшек и других носителей в работе с компьютерами организации, а также передача информационных данных об организации посторонним людям

Д) Вся история действий сотрудников на компьютере, хранится в базе данных отдела по Информационной безопасности

3. Физическая безопасность (доступ в помещение)

3.1. Все объекты критичные с точки зрения информационной безопасности (все сервера баз данных, телефонная станция, основной маршрутизатор, файервол) находятся в

отдельном помещении, доступ в которое разрешен только сотрудникам, имеющими соответствующее разрешение от руководства организации.

3.2. Вход в помещение осуществляется через металлическую дверь, оснащенную замками и переговорным устройством. Также перед входом стоит охранник для записи всех сотрудников посетивших это помещение.

3.3. Помещение оборудовано принудительной вентиляцией и пожарной сигнализацией. Вход в помещение контролируется системой видео наблюдения с выходом на мониторы охраны.

3.4. Ключевые дискеты, пароли и прочая конфиденциальная информация хранится в сейфах.

3.5. Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находится в помещении только в присутствии работников, имеющих право находится в помещении в связи с выполнением своих должностных обязанностей.

4. Работа в глобальной сети Интернет.

4.1 К работе с ресурсами сетью Интернет допускаются сотрудники, получившие соответствующее разрешение от руководства.

4.2 Работа сотрудников организации с электронной почтой сети Интернет допускается на основании отдельного разрешения от руководства организации.

4.3 При работе с сетью Интернет сотрудникам запрещено:

· Скачивать и устанавливать на компьютер программное обеспечение.

· Посещать ресурсы, не имеющие непосредственного отношения к работе и служебным обязанностям.

· Осуществлять подписку на рассылку информации непроизводственного характера.

· Сообщать адрес электронной почты в непроизводственных целях.

· Использовать Интернет для развлечения .

Технический регламент

Общие положения :

* Настоящий регламент определяет профилактические меры для предотвращения утечки информации
* Данный регламент действует на всех работников «ПАРАВОЗ» имеющих доступ к внутренней сети компании
* исключать возможность доступа третьих лиц к документам, содержащим конфиденциальную информацию;
* не использовать чужие средства идентификации и не передавать никому свои, не входить в систему под чужим логином;
* соблюдать установленные уровни допуска к информации;
* не переписывать на съемные носители конфиденциальные данные без санкции руководителя, не передавать их по любым каналам связи, не раскрывать лицам, не имеющим соответствующего уровня доступа;
* соблюдать требования и правила по работе со средствами технической защиты, в том числе со средствами криптографической защиты;
* контролировать состояние автоматизированного рабочего места, сообщать СБ обо всех ситуациях, имеющих характер инцидентов информационной безопасности, а именно: нарушении целостности пломб, свидетельствующем о попытке проникнуть в охраняемую зону, некорректном срабатывании антивирусной защиты, нарушениях в работе программного обеспечения, выявленных изменениях файлов, выходе из строя периферийных устройств;
* обеспечивать отсутствие на своем АРМ самостоятельно установленных программ;
* исключать копирование любых файлов или текстовой информации в любых целях без получения санкции руководителя.

Определения:

* СБ- служба безопасности
* APM - **Автоматизи́рованное рабо́чее ме́сто** (АРМ) — программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида
* ПД-персональные данные

**Безопасность персональных данных**

* **Для доступа к информационным ресурсам и к обработке файлов у сотрудника должно быть разрешение для обработки данной информации**
* **работник должен знать нормативно-правовые акты**,
* **действия, которые запрещены сотруднику**, допущенному к обработке ПД. Вносить изменения в конфигурацию компьютера или в программные продукты, обрабатывать персональные данные в присутствии третьих лиц, оставлять на рабочем месте документы или электронные носители информации, содержащие ПД, использовать ошибки в программах для распространения или изменения ПД

**Должностная инструкция начальника отдела по защите информации**

I. Общие положения

1. Начальник отдела по защите информации относится к категории руководителей.

2. На должность начальника отдела по защите информации назначается лицо, имеющее высшее профессиональное (техническое) образование и стаж работы по защите информации на инженерно-технических и руководящих должностях не менее 3 лет.

3. Назначение на должность начальника отдела по защите информации и освобождение от нее производится приказом директора предприятия.

4. Начальник отдела по защите информации должен знать:

4.1. Действующее законодательство о государственной и коммерческой тайне и защите информации.

4.2. Постановления правительства, определяющие основные направления экономического и социального развития отрасли.

4.3. Руководящие, нормативные и методические материалы по вопросам, связанным с обеспечением защиты информации.

4.4. Перспективы развития, специализацию и направления деятельности предприятия и его подразделений.

4.5. Характер взаимодействия подразделений в процессе исследований и разработок и порядок прохождения служебной информации.

4.6. Организацию комплексной защиты информации в отрасли, на предприятии.

4.7. Перспективы и направления развития технических средств защиты информации.

4.8. Методы и средства контроля охраняемых сведений, выявления каналов утечки информации, организацию технической разведки.

4.9. Порядок финансирования, методы планирования и организации проведения научных исследований и разработок, выполнения работ по защите информации.

4.10. Порядок заключения договоров на проведения специальных исследований и проверок, работ по защите технических средств передачи, обработки, отображения и хранения информации.

4.11. Основы трудового законодательства.

4.12. Правила и нормы охраны труда.

5. Начальник отдела по защите информации в своей деятельности руководствуется:

5.1. Положением об отделе по защите информации.

5.2. Настоящей должностной инструкцией.

6. Начальник отдела по защите информации подчиняется непосредственно

7. На время отсутствия начальника отдела по защите информации (командировка, отпуск, болезнь, пр.) его обязанности исполняет заместитель (при отсутствии такового - лицо, назначенное в установленном порядке), который приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

II. Должностные обязанности

Начальник отдела по защите информации:

1. Организует разработку и внедрение организационных и технических мероприятий по комплексной защите информации на предприятии, ведущем работы, содержание которых составляет государственную или коммерческую тайну, обеспечивает соблюдение режима проводимых работ и сохранение конфиденциальности документированной информации.

2. Возглавляет разработку проектов перспективных и текущих планов работы, составление отчетов об их выполнении.

3. Руководит проведением работ по организации, координации, методическому руководству и контролю их выполнения по вопросам защиты информации и разработкой технических средств контроля, определяет перспективы их развития.

4. Обеспечивает взаимодействие и необходимую кооперацию соисполнителей работ по вопросам организации и проведения научно-исследовательских и опытно-конструкторских разработок, организует и контролирует выполнение плановых заданий, договорных обязательств, а также сроки, полноту и качество работ, выполняемых соисполнителями.

5. Организует работу по заключению договоров на работы по защите информации, принимает меры по обеспечению финансирования работ, в том числе выполняемых по договорам.

6. Обеспечивает участие подразделения в разработке технических заданий на выполняемые на предприятии исследования и разработки, формулирует цели и задачи работы по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации.

7. Организует проведение специальных исследований и контрольных проверок по выявлению демаскирующих признаков и возможных каналов утечки информации, в том числе по техническим каналам, разрабатывает меры по их устранению и предотвращению, а также работу по составлению актов и другой технической документации о степени защищенности технических средств и помещений.

8. Контролирует соблюдение нормативных требований по надежной защите информации, обеспечивает комплексное использование технических средств, методов и организационных мероприятий.

9. Организует рассмотрение применяемых и предлагаемых методов защиты информации, промежуточных и конечных результатов исследований и разработок.

10. Совершенствует планирование, контроль и организацию выполнения работ, обеспечивает использование в них достижений отечественной и зарубежной науки и техники, передового опыта.

11. Обеспечивает выполнение плановых заданий с наименьшими затратами материальных и финансовых ресурсов, рациональное расходование фонда заработной платы.

12. Согласовывает проектную и другую техническую документацию на вновь строящиеся и реконструируемые здания и сооружения в части выполнения требований по защите информации.

13. Определяет потребность подразделения в оборудовании, материальных, финансовых и трудовых ресурсах, необходимых для проведения работ, и контролирует рациональное использование и сохранность аппаратуры. Приборов и другого оборудования.

14. Обеспечивает высокий научно-технический уровень работ, эффективность и качество исследований и разработок.

15. Осуществляет контроль за выполнением предусмотренных мероприятий, анализ материалов контроля выявления нарушений, разрабатывает и участвует в реализации мер по устранению выявленных недостатков по защите информации.

16. Организует проведение аттестации объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты информации по соответствующим классам безопасности, обеспечивает представление в установленном порядке действующей отчетности.

17. Участвует в подборе кадров, оценке деятельности и аттестации работников подразделения.

18. Определяет направления деятельности подразделений, входящих в состав отдела, организует и координирует их работу.

19. Осуществляет рациональную расстановку кадров с учетом квалификации и деловых качеств работников, принимает меры по повышению их квалификации и творческой активности.

20. Обеспечивает ведение делопроизводства в соответствии с установленным порядком, соблюдение действующих инструкций по режиму работ и своевременно принимает меры по предупреждению нарушений.

21. Следит за безопасным проведением работ, соблюдением правил и норм охраны труда.

22. Руководит работниками подразделения.

**III. Права**

Начальник отдела по защите информации вправе:

1. Знакомиться с проектами решений руководства предприятия, касающимися деятельности отдела.

2. Осуществлять взаимодействие с руководителями всех структурных подразделений организации по вопросам защиты информации.

3. Подписывать документы в пределах своей компетенции.

4. Вносить на рассмотрение руководства предприятия:

4.1. Представления о назначении, перемещении и освобождении от занимаемых должностей подчиненных ему работников.

4.2. Предложения:

- о поощрении отличившихся работников;

- привлечении к материальной и дисциплинарной ответственности виновных в утечке информации, составляющей государственную и коммерческую тайну.

5. Требовать от руководства предприятия оказания максимального содействия в исполнении своих должностных обязанностей и прав.

6. Запрашивать и получать от руководителей структурных подразделений предприятия, специалистов и рабочих информацию и материалы, необходимые для организации работы отдела.

**IV. Ответственность**

Начальник отдела по защите информации несет ответственность:

1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией - в пределах, определенных действующим трудовым законодательством Российской Федерации.

2. За правонарушения, совершенные в процессе осуществления своей деятельности - в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

3. За причинение материального ущерба - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.