5.7.5. При обнаружении на носителе информации или в полученных файлах программ вирусов пользователи докладывают об этом ответственному сотруднику, и принимают меры восстановлению работоспособности программных средств и данных.

О факте обнаружения программных вирусов сообщается в орган, от которых поступили зараженные файлы, для принятия мер по локализации и устранению программных вирусов.

Перед отправкой массивов информации и программных средств, осуществляется ее проверка на наличие программных вирусов.

При обнаружении программных вирусов пользователь обязан немедленно прекратить все работы на АРМ, принять меры к их локализации и удалению с помощью имеющихся антивирусных средств защиты.

5.7.6. Организация антивирусной защиты конфиденциальной информации должна быть направлена на предотвращение заражения компьютеров, входящих в состав локальных компьютерных сетей, и серверов различного уровня и назначения вирусами.

5.7.7. Необходимо постоянно осуществлять обновление вирусных баз. Частоту обновления установить в зависимости от используемых антивирусных средств и частоты выпуска обновления указанных баз.

5.7.8. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке, руководством по эксплуатации конкретного антивирусного программного продукта и инструкцией по антивирусной защите.

5.8. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на ответственного специалиста.

5.8.1. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

– длина пароля должна быть не менее 8 символов;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения;

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

– личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5.8.2 Формирование личных паролей пользователей осуществляется централизованно. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других сотрудников подразделений.

5.8.3. Полная плановая смена паролей пользователей должна проводиться регулярно.

5.8.4. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться по представлению уполномоченными сотрудниками немедленно после окончания последнего сеанса работы данного пользователя с системой.

5.8.5. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с п.5.8.4 настоящего Положения.

5.8.6 Хранение сотрудником (исполнителем) значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя в опечатанном конверте.

5.8.7. Периодический контроль за действиями исполнителей при работе с паролями, соблюдением порядка их смены и использования возлагается на ответственного сотрудника.

6. Обязанности и права должностных лиц

6.1. Руководство технической защитой конфиденциальной информации в ООО «КАДРОВЫЙ ОПЕРАТОР ВАКАНСИЯ 22» возлагается на руководителя.

6.2. Специалист по обслуживанию вычислительной техники организуют и обеспечивают техническую защиту информации, циркулирующую в технических средствах и помещениях.

6.3. Ответственный сотрудник по технической защите конфиденциальной информации осуществляет непосредственное руководство разработкой мероприятий по технической защите конфиденциальной информации и контролю.

6.4. Пользователи ОТСС обеспечивают уровень технической защиты информации в соответствии с требованиями (нормами), установленными в нормативных документах.

6.5. Владельцы и пользователи ОТСС обязаны вносить предложения о приостановке работ с использованием сведений, составляющих конфиденциальную или служебную тайну, в случае обнаружения утечки (или предпосылок к утечке) этих сведений. Предложения докладываются руководителю.

6.6. Руководитель имеет право привлекать к проведению работ по технической защите конфиденциальной информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

7. Планирование работ по технической защите конфиденциальной информации и контролю.

7.1. В ООО «КАДРОВЫЙ ОПЕРАТОР ВАКАНСИЯ 22» составляется годовой план работ по технической защите конфиденциальной информации и контролю ответственным сотрудником, выполняющими работы с защищаемой. Сроки разработки, представления и утверждения планов устанавливаются руководителем.

7.2. В годовые планы по технической защите конфиденциальной информации и контролю включаются:

мероприятия по выполнению постановлений и распоряжений по вопросам защиты конфиденциальной информации;

подготовка проектов распорядительных документов по вопросам организации технической защиты информации, инструкций, рекомендаций, памяток и других документов по обеспечению безопасности информации при использовании конкретных технических средств обработки и передачи информации, на автоматизированных рабочих местах, в ЗП;

аттестация вводимых в эксплуатацию ОТСС и ЗП, а также периодическая переаттестация находящихся в эксплуатации ОТСС и ЗП на соответствие требованиям по технической защите конфиденциальной информации;

проведение периодического контроля состояния технической защиты информации;

мероприятия по устранению нарушений и выявленных недостатков по результатам контроля;

мероприятия по совершенствованию технической защиты информации.

7.3. Контроль выполнения планов и отчетность по ним возлагается на директора.

8. Контроль состояния технической защиты конфиденциальной информации.

8.1. Основными задачами контроля состояния технической защиты конфиденциальной информации являются оценка уровня и эффективности, принятых мер защиты, своевременное выявление и предотвращение утечки по техническим каналам информации, составляющей конфиденциальную или служебную тайну, НСД к информации, преднамеренных программно-технических воздействий на информацию с целью ее уничтожения, искажения, блокирования, нарушения правового режима использования информации.

8.2. Контроль осуществляется – не реже 1 раза в год;

Ответственным сотрудником и пользователем – непрерывно.

8.3. Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты конфиденциальной информации, решений ФСТЭК России, постановлений и распоряжений вышестоящих органов, наличия соответствующих документов по технической защите конфиденциальной информации, в инструментальной и визуальной проверке ОТСС и ЗП на наличие каналов утечки информации, на соответствие требованиям и нормам технической защиты информации.

9. Аттестация рабочих мест

9.1. Аттестации на соответствие требованиям по технической защите конфиденциальной