Приложение №8 к приказу от 04.03.2022 №31-О

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ

администратора безопасности информационных систем персональных данных

1. Общие положения

1.1. Настоящая инструкция предназначена для Администратора безопасности Информационной системы персональных данных (далее ИСПДн), назначенного для администрирования средств и механизмов защиты, реализующих требования по обеспечению информационной безопасности в ИСПДн муниципального бюджетного учреждения «Централизованная библиотечная система» (далее – Учреждение).

1.2. Администратор безопасности ИСПДн и исполняющий обязанности в его отсутствие, назначаются приказом руководителя Учреждения из числа сотрудников, имеющих достаточную квалификацию и опыт работы со средствами вычислительной техники (далее СВТ) и допущенными ко всей обрабатываемой в данной ИСПДн информации.

1.3. Администратор безопасности ИСПДн, в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных (далее ПДн), обрабатываемых при помощи СВТ в ИСПДн Учреждения.

1.4. Администратор безопасности ИСПДн непосредственно подчиняется руководителю Учреждения.

1.5. В своей работе Администратор безопасности ИСПДн руководствуется действующим законодательством РФ, нормативными актами органов государственной власти, настоящей инструкцией, нормативными актами органов государственной власти, Положением о порядке обработки ПДн в ИСПДн, Положением о ПДн, Требованиями по обеспечению ИБ ИСПДн, настоящей Инструкцией, а также другими нормативными документами.

2. Обязанности администратора безопасности ИСПДн

Администратор безопасности ИСПДн обязан:

2.1. Соблюдать Требования по обеспечению информационной безопасности информационной системы персональных данных Парус- Кадры и штатное расписание, Парус - Бухгалтерский учет, Парус- Управление закупками, ИРБИС (ИСПДн) установленные Учреждением.

2.2. Обеспечить выполнение защитных мер предусмотренных Требованиями по обеспечению информационной безопасности информационной системы персональных данных Парус- Кадры и штатное расписание, Парус - Бухгалтерский учет, Парус- Управление закупками, ИРБИС (ИСПДн).

2.3. Организовывать проведение работ по обслуживанию средств защиты информации.

2.4. Выявлять попытки несанкционированного доступа к защищаемой информации и участвовать в проведении служебных расследований по фактам выявленных нарушений в ИСПДн.

2.5. Проводить обучение и консультирование пользователей ИСПДн Учреждения правилам работы с используемыми средствами защиты информации.

2.6. Проводить работы по выявлению угроз и уязвимостей при обработке ПДн в ИСПДн Учреждения с учетом специфики конкретной ИСПДн и применяемых средств защиты.

2.7. Готовить предложения по совершенствованию применяемой системы защиты информации и ее отдельных компонентов.

2.8. Распределять между пользователями ИСПДн необходимые реквизиты используемых средств защиты информации.

2.9. Принимать участие в санкционированной установке и изменении эксплуатируемого в ИСПДн программного обеспечения (совместно со специалистами, обслуживающими ИСПДн).

2.10. Поддерживать актуальность соответствующей нормативно-справочной информации, необходимой для работы пользователей.

2.11. Участвовать в проведении служебных расследований фактов нарушения функционирования ИСПДн, целостности программного обеспечения, а также других случаев нарушения правил обработки защищаемой информации.

2.12. В необходимых случаях проводить контроль технологического процесса обработки информации в ИСПДн специальными средствами программного контроля с целью выявления несанкционированных действий пользователей.

2.13. Совместно со специалистами, обслуживающими ИСПДн, принимать участие в работах по восстановлению работоспособности ИСПДн в случаях компрометации паролей, ключей, а также в других нештатных ситуациях, принимать меры по восстановлению работоспособности средств и систем защиты информации.

2.14. Осуществлять постоянный контроль за соблюдением правил хранения реквизитов средств защиты информации.

2.15. Контролировать работу пользователей со средствами защиты информации.

2.16. Проверять отсутствие вредоносных программ на используемых в ИСПДн съёмных носителях информации.

2.17. Осуществлять постоянный контроль над правильностью функционирования ИСПДн и функционирования системы защиты информации в ИСПДн.

2.18. Контролировать состав аппаратных средств и программного обеспечения СВТ.

2.19. Поддерживать в актуальном состоянии техническую и эксплуатационную документацию на средства защиты информации в ИСПДн.

2.20. Осуществлять контроль состава пользователей ИСПДн и их полномочий.

2.21. Поддерживать в актуальном состоянии список лиц допущенных к обработке ПДн в ИСПДн Учреждения, а также перечень помещений, в которых осуществляется обработка ПДн.

2.22. Немедленно докладывать непосредственному руководству подразделения обо всех выявленных нештатных ситуациях в ИСПДн, а также принимать необходимые меры по устранению нарушений.

2.23. Своевременно осуществлять смену ключевой информации средств защиты.

2.24. Оказывать содействие работникам УИТ в проведении работ по анализу защищенности ИСПДн.

2.25. Постоянно повышать свою квалификацию в области защиты информации, в совершенстве знать правила эксплуатации используемых средств защиты информации.

2.26. Своевременно информировать пользователей об изменениях, вносимых в систему защиты информации.

2.27. Проводить антивирусную проверку после установки (изменения) системного и прикладного программного обеспечения на рабочих станциях ИСПДн.

2.28. Следить за сохранностью наклеек с защитной и идентификационной информацией на корпусах ПЭВМ;

2.29. Знать уровень конфиденциальности обрабатываемой информации и класс ИСПДн, следить за тем, чтобы обработка информации производилась только с использованием учтенных съемных и несъемных носителей информации;

2.30. Контролировать соблюдение требований по учету и хранению носителей конфиденциальной информации и персональных данных;

2.31. Контролировать правильность применения пользователями сети средств защиты информации.

2.32. Участвовать в испытаниях и проверках ИСПДн.

2.33. Не допускать к работе на рабочих станциях и серверах ИСПДн Учреждения посторонних лиц.

2.34. Осуществлять контроль монтажа оборудования Учреждения участвующего в ИСПДн специалистами сторонних организаций.

2.35. Обобщать результаты своей деятельности и готовить предложения по ее совершенствованию.

2.36. Не реже одного раза в три месяца Администратор безопасности ИСПДн осуществляет контроль за отключением и обновлением антивирусных средств на всех автоматизированных рабочих местах и серверах ИСПДн. Результаты контроля должны быть сохранены в Журнале инцидентов и изменений конфигураций вычислительной системы банка.

2.37. Администратор безопасности ИСПДн не реже одного раза в три месяца осуществляет анализ журналов регистрации событий на автоматизированных рабочих местах и серверах ИСПДн. Результаты анализа Администратор безопасности ИСПДн сохраняет в Журнале инцидентов и изменений конфигураций вычислительной системы банка.

2.38. Администратор безопасности ИСПДн осуществляет сохранение параметров конфигурации средств защиты и механизмов защиты информации от НСД на неизменяемом носителе, который размещается на хранение в сейф УИТ (CD-ROM или DVD-ROM с закрытой сессией записи).

2.39. Не реже одного раза в год Администратор безопасности ИСПДн осуществляет сравнение параметров конфигурации средств защиты и механизмов защиты информации от НСД с данными сохраненными на неизменяемом носителе (CD-ROM или DVD-ROM с закрытой сессией записи) находящемся в сейфе УИТ. Результаты проверки должны фиксироваться в Журнале инцидентов и изменений конфигураций вычислительной системы Учреждения.

3. Правила парольной защиты

3.1. Пароли формируются самостоятельно пользователями ИСПДн Учреждения или Администратором безопасности ИСПДн.

3.2. Пользователь ИСПДн имеет право самостоятельно изменять свой пароль.

3.3. Смена пароля должна происходить в обязательном порядке не реже одного раза в шесть месяцев.

3.4. Длина используемого пароля не может быть менее шести алфавитно-цифровых символов.

3.5. Свой пароль пользователь ИСПДн не имеет права сообщать никому.

3.6. В случае необходимости использования учетной записи отсутствующего работника Администратор безопасности ИСПДн может произвести установку нового пароля и передать его замещающему сотруднику на основании служебной записки оформленной руководителем подразделения.

3.7. Внеплановые удаление или смена пароля пользователя ИСПДн Учреждения в случае прекращения или любого изменения его полномочий должны производиться немедленно после окончания последнего сеанса работы данного пользователя. При этом должна быть также выполнена безотлагательная корректировка прав доступа на всех средствах вычислительной техники в соответствии с изменившимися полномочиями работника.

3.8. Внеплановая полная смена паролей должна производиться в случае прекращения полномочий Администраторов безопасности ИСПДн, Администраторов ИСПДн и других работников, которым по роду работы были предоставлены полномочия по управлению ИСПДн Учреждения.

4. Правила антивирусной защиты

4.1. Все рабочие места с которых осуществляется работа в ИСПДн должны быть защищены антивирусными средствами.

4.2. Установка и обновление антивирусных средств используемых на автоматизированных рабочих местах и серверах ИСПДн должны контролироваться Администратором безопасности ИСПДн.

4.3. Программное обеспечение устанавливаемое или изменяемое на автоматизированных рабочих местах и серверах ИСПДн должно быть предварительно проверено на отсутствие вирусов. После установки или изменения программного обеспечения должна быть также выполнена антивирусная проверка. Результаты установки, изменения программного обеспечения и антивирусной проверки на автоматизированных рабочих местах и серверах ИСПДн должны быть сохранены в Журнале инцидентов и изменений конфигураций вычислительной системы банка.

4.4. Установка или изменение программного обеспечения на автоматизированных рабочих местах и серверах ИСПДн должна происходить только по согласованию и под контролем Администратора безопасности ИСПДн.

4.5. Не реже одного раза в три месяца Администратор безопасности ИСПДн осуществляет контроль за отключением и обновлением антивирусных средств на всех автоматизированных рабочих местах и серверах ИСПДн. Результаты контроля должны быть сохранены в Журнале инцидентов и изменений конфигураций вычислительной системы банка.

5. Права администратора безопасности ИСПДн

Администратор безопасности ИСПДн имеет право:

5.1. Реализация требований по обеспечению безопасности персональных данных в ИСПДн должна осуществляться по согласованию и под контролем Администратора безопасности ИСПДн.

5.2. Требовать от пользователей вверенной ИСПДн безусловного соблюдения установленной технологии обработки информации и неукоснительного выполнения требований информационной безопасности.

5.3. Обращаться к руководству структурных подразделений Учреждения с требованием о прекращении обработки информации в ИСПДн в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации в соответствующем подразделении.

5.4. Взаимодействовать со специалистами, обеспечивающими техническое обслуживание и сопровождение программных средств ИСПДн.

5.5. Обращаться к специалистам, обеспечивающим техническое обслуживание и сопровождение программных средств ИСПДн с просьбами об оказании необходимой технической и методической помощи в работе по обеспечению безопасности информации, по вопросам внедрения и эксплуатации средств и систем защиты информации.

6. Ответственность администратора безопасности ИСПДн

Администратор безопасности ИСПДн несет ответственность:

6.1. За соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации.

6.2. За разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.