**Наименование предприятия:** ООО «Транснефть – Дальний Восток», отдел информационных технологий.

**Направление обучения участников:** Обеспечение информационной безопасности автоматизированных систем.

**Название кейса:** Разработка Технического задания (ТЗ) на разработку автоматизированной системы в соответствии с типовые требования в части защиты информации от несанкционированного доступа (НСД).

**Описание:**

Цель проекта:

Разработать автоматизированную систему принятия решения «Подбор кандидатов на открытую вакансию», автоматизировать процесс поиска кандидатов на сайтах вакансий, с целью уменьшения времени на поиск кандидатов на замещение вакантных должностей.

Требования к автоматизированной системе принятия решений (АС ПР):

1. Дружественный WEB интерфейс;

2. Личный кабинет руководителя-нанимателя, в котором осуществляется формирование заказа на подбор в одно из подразделений компании, и отображается статус поиска/оформления кандидата;

3. Ввод требований и контрольных вопросов к кандидатуре соискателя

4. Возможность интеграции с корпоративной ERP;

5. Учесть корпоративные и государственные требования по соблюдению информационной безопасности и защищённости персональных данных **(в соответствии с приложенными типовыми требованиями**);

6. Автоматический поиск на открытых интернет ресурсах(HH.RU), подходящих кандидатов, на основе указанных требования;

7. Автоматическая публикация вакансий на сайте hh.ru по заданным руководителем параметрам;

8. Автоматическое первичное тестирование отобранных кандидатов, предоставление результатов в отдел кадров;

9. Аккумуляция все собранной информации по кандидатам;

9. Направление отобранного кандидата на согласование руководством по средствам СЭД;

10. Направление данных о согласованном кандидате в корпоративную ERP.

11. Автоматическое назначение собеседования с руководителем с возможностью переноса и автоматического оповещения второй стороны.

12. Автоматический отчет «воронка» отображающий сквозные показатели в разрезе времени и конверсии кандидатов с группировкой по руководителям-нанимателям. Отчет должен позволять оценить эффективность процесса и увидеть узкие места.

**Задание:** Разработать Техническое задание (ТЗ) на разработку в соответствии с требованиями ГОСТ 34\*, приложенных Типовых требования для ТЗ в части защиты информации от несанкционированного доступа, на основании цели проекта и требований к разрабатываемой АС.

**Типовые требования для Технического задания (ТЗ) в части защиты информации от несанкционированного доступа (НСД).**

**В раздел ТЗ «Требования по защите информации от НСД» включаются следующие требования:**

1. Разработка информационной системы (далее – ИС) должна производиться с учетом требований настоящего документа.
2. В соответствии с техническими требованиями на создание ИС, в техническом задании должны быть детализированы требования к функциям, реализуемым в части ИБ.
3. В части управления доступом ИС должна обеспечивать:

* идентификацию и аутентификацию пользователей ИС при доступе к системе. Пароли не должны храниться и передаваться по сети в рамках процедур аутентификации в открытом виде;
* ограничение количества неуспешных попыток аутентификации в ИС, после которых учетная запись должна быть заблокирована;
* управление идентификаторами (учетными записями пользователей), в том числе создание, присвоение, уничтожение идентификаторов;
* управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
* защита обратной связи при вводе аутентификационной информации;
* разграничение прав доступа к отдельным операциям, отчетам, данным (например, выполнение, просмотр, изменение, создание, удаление, просмотр изменений и др.), функциям ИС на основе ролей пользователей, наборов полномочий;
* контроль предоставляемых ролей и наборов полномочий пользователей ИС и отсутствия их функционального пересечения;
* контроль доступа пользователей к защищаемым ресурсам информационной системы в соответствии с правами доступа.

1. В части регистрации и учета событий ИБ ИС должна обеспечивать:

* регистрацию входа (выхода) пользователей в ИС (из ИС). В параметрах регистрации должно указываться:

дата и время входа (выхода) пользователей в ИС (из ИС);

идентификатор пользователя, предъявленный при запросе доступа;

результат попытки входа: успешная или неуспешная;

идентификатор (адрес) с которого осуществлялся вход в ИС.

* регистрацию изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации должно указываться:

дата и время изменения полномочий доступа;

идентификатор пользователя, осуществившего изменение;

прежнее и измененное значение полномочий доступа (при технической возможности).

* регистрацию действий пользователей и администраторов в ИС. В параметрах регистрации должно указываться:

дата и время регистрируемого события;

идентификатор (код) субъекта доступа;

идентификатор (код) объекта доступа;

выполняемое действие.

1. В части обеспечения целостности ИС должна обеспечивать:

* автоматическую проверку целостности программной среды ИС и программных СЗИ по контрольным суммам файлов ИС при загрузке системы и в процессе функционирования ИС, а также по требованию администратора системы и куратора ИБ. По результатам автоматического контроля целостности в случае изменения контрольных сумм файлов ИС должно направляться уведомление администратору системы и куратору ИБ. Объем и состав контролируемых данных должен быть описан в проектных решениях;
* периодическое резервное копирование настроек ИС и СЗИ и их восстановление;

выполнение установки обновлений безопасности ОС и прикладного ПО. На этапах предварительных и приемочных испытаний должны быть продемонстрированы компоненты ИС с установленными актуальными обновлениями б