ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

*Московский институт электроники и математики им. А.Н.Тихонова*

**Задание по теме 8. Международные и отраслевые стандарты.   
Стандарт ISO/IEC 27001**

По направлению 10.04.01 – «Информационная безопасность»

Проверил:

преп. Новожилов П.

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил:

Новиков В. С. МКБ 241

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Москва 2024

# Задание

**Исходные данные**

Кадровое агентство рассматривает получение сертификата по российскому стандарту ГОСТ Р 27001-2021.

В организацию пришел новый руководитель ИБ-подразделения и провел GAP-анализ, по результатам которого выявил:

* Доступ предоставляется по сложившимся практикам, без заявок;
* Работники подбора персонала подключаются в систему под групповой учетной записью;
* Отсутствует документация в области ИБ;
* Информация по инцидентам заносится в разные источники в свободной форме (представитель ИТ указывает информацию по своим типам, работники ИБ указывают свою информацию, которая отличается от работников из ИТ-подразделения);
* Не выстроен процесс управления уязвимостями, в том числе в части собственной разработки прикладных систем, реализующих бизнес-процесс;
* Управление изменениями конфигураций в информационных системах, входящих в область действия стандарта, осуществляется без заявок;
* Консоль для удаленного доступа к личному кабинету, входящему в область действия стандарта, доступному в сеть Интернет, осуществляется без использования каких-либо средств защиты информации. Удалённый доступ предоставляется хаотично без каких-либо процедур/заявок;
* Передача персональных данных соискателей клиентам осуществляется через сеть Интернет без использования средств шифрования;
* В одном сетевом сегменте локально-вычислительной сети размещены пользователи, серверы, администраторы.

# Решение

Таблица 1. Определение несоответствия требованиям стандарта ГОСТ Р 27001-2021

|  |  |  |
| --- | --- | --- |
| № | Описание выявленного  несоответствия | Ссылка на пункт стандарта ГОСТ Р 27001-2021 |
| 1 | Политики информационной безопасности (отсутствуют документы в области ИБ) | A.5.1.1 |
| 1.1 | Пересмотр политик информационной безопасности (отсутствуют документы в области ИБ) | A.5.1.2 |
| 1.2 | Дополнительно: осведомленность сотрудников о политиках ИБ | A.7.2.2 |
| 2 | Удалённый доступ предоставляется хаотично без каких-либо процедур/заявок. Нет регламента по удаленной работе | A.6.2.2 |
| 2.1 | Дополнительно: отсутствуют требования к использованию средств криптографической защиты (A.10.1.1) для доступа к удаленным ресурсам | A.10.1. |
| 2.2 | Дополнительно: внедрить процесс идентификации и аутентификации пользователей при удаленной работе | A.9.2.4 |
| 3 | Отсутствует политика управления доступом.  Доступ предоставляется без заявок и обоснования | A.9.1.1 |
| 3.1 | Дополнительно: внедрить процесс регулярного пересмотра прав доступа | A.9.2.5 |
| 3.2 | Дополнительно: организовать меры по управлению привилегированным доступом | A.9.2.3 |
| 4 | Нет единого управления сбора инцидентов ИТ/ИБ. Информация по инцидентам заносится в разные источники в свободной форме. | A.16.1 |
| 4.1 | Не разработан формализованный процесса анализа и классификации инцидентов | A.16.1.4 |
| 4.2 | Дополнительно: организовать процесс обучения сотрудников по выявлению и сообщению о событиях ИБ | A.16.1.2, A.16.1.3 |
| 6 | Не выстроен процесс управления уязвимостями. Нет оценки влияния уязвимостей на бизнес-процесс | A.12.6.1 |
| 7 | Процесс управления изменениями. Не выстроен hardering, процесс контроля состояния системы. Не учитываются изменения в системе. | A.12.1.2 |
| 7.1 | Не выстроен hardering, процесс управления конфигурациями для приложений и оборудования. Не учитываются изменения в ПО. | A.12.5.1 |
| 7.2 | Дополнительно hardering: отсутствует регламент тестирования изменений перед их внедрением в эксплуатацию | A.14.2.2 |
| 8 | Отсутствует сегментация сетей. Все в одном сетевом сегменте локально-вычислительной сети. | А.13.1.3 |
| 8.1 | Дополнительно: скорее всего отсутствует контроль доступа к сетям с использованием VLAN | A.9.1.2 |
| 9 | Не регламентированы процедуры передачи информации | A.13.2.1 |
| 10 | Отсутствуют соглашения о передаче информации | A.13.2.2 |
| 11 | Передача персональных данных соискателей клиентам осуществляется через сеть Интернет без использования средств шифрования | A.13.2.3 |
| 11.1 | Дополнительно: нет регламента хранения и уничтожения данных после передачи | A.8.3.2 |