МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ЧЕЛЯБИНСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КАТАВ-ИВАНОВСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ»

ПРИНЯТО
На заседании Совета техникума
ГБПОУ «К-ИИТ»
Протокол № 69
от 30.12 2015 г.

УТВЕРЖДАЮ
Директор ГБПОУ «К-ИИТ»
_____ Болотникова Н.В.
Приказ № 423/08
от 30.12. 2015 г.

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Общие положения

1.1. Настоящий положение определяет информационную безопасность ГБПОУ «Катав-Ивановского индустриального техникума» (далее – техникум).

К объектам информационной безопасности техникума относят:

- информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
- средства и системы информатизации – средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

2. О системном администрировании и обязанностях ответственного за информационную безопасность

2.1 Задачи связанные с мерами системного администрирования, обеспечивающего информационную безопасность являются частью работы инженера по защите информации.

2.2 Для решения задач информационной безопасности инженера по защите информации должен:

2.3 Следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);

2.4 Обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;

2.5 Обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;

2.6 Обеспечивать нормальное функционирование системы резервного копирования.

3. Базы данных

3.1 Базы данных подлежащие защите вносятся в «Реестр баз данных подлежащих информационной защите». Форма реестра – Приложение 1.

Для каждой базы данных включенной в «Реестр баз данных подлежащих информационной защите» приказом директора техникума по представлению Комиссии по информационной безопасности должен назначаться Ответственный за ведение базы данных.

3.2 Все процедуры по использованию и обслуживанию баз данных осуществляет Ответственный за ведение базы данных. В том числе:

- резервное копирование;
- периодический контроль исправности резервных копий;

- подключение и отключение пользователей;
- внесение изменений в структуру базы, а также изменений в «Реестр баз данных подлежащих информационной защите», при необходимости (изменение степени конфиденциальности, места расположения и т.д.);
- прочие виды работ связанных с данной базой.

3.3 Все изменения «Реестра баз данных подлежащих информационной защите» осуществляется по решению Комиссии по информационной безопасности, состоящей из директора техникума, ответственного за информационную безопасность, ответственного за информационную безопасность, ответственного за ведение базы данных.

3.4 В случае если база данных требует парольной защиты, то ответственный за базу данных руководствуется требованиями раздела 4 «Система аутентификации» настоящего документа.

4. Система аутентификации

4.1 На всех клиентских ПК используется WINDOWS XP PROFESSIONAL, WINDOWS 7, WINDOWS 8, Red Hat Enterprise Linux 6 (LinuxWizard).

4.2 Для использования локальной вычислительной сети в учебном процессе используются групповая идентификация: пользователь - обучающийся, преподаватель, администратор с разграничением прав доступа к папкам файлового сервера.

4.3 Для всех пользователей баз данных устанавливаются уникальные пароли.

4.4 Периодичность плановой смены паролей 1 раз в начале учебного года.

4.5 Установить блокировку учетной записи пользователей при неправильном наборе пароля более трёх раз.

4.6 Вести журнал назначения и смены паролей единый для всех баз данных.

4.7 Обязать пользователей осуществлять выход из базы данных, если планируется отсутствие на рабочем месте.

4.8 Обязать пользователей не разглашать сетевые реквизиты (имена и пароли) для доступа к информационным ресурсам, а также хранить их в недоступном месте.

4.9 Обслуживание системы аутентификации осуществляют ответственные за базы данных.

5. Защита по внешним цифровым линиям связи

5.1 В целях уменьшения риска повреждения программного обеспечения и утери информации, доступ из внутренней сети во внешнюю (Интернет, электронная почта) осуществляется через компьютеры с установленными брэндмауэром и антивирусом.

5.2 Запрещено несанкционированное использование модемов или иных средств доступа с ПК, подключенных к внутренней сети, во внешние сети.

5.3 Подключение рабочих станции техникума к внешним линиям связи производится в локальной вычислительной сети по протоколам Ethernet и WiFi.

5.4 Защита от несанкционированного подключения к ЛВС и размещение активного сетевого оборудования.

5.5 Сервер размещается в специально выделенной серверной и имеет ограниченный доступ.

5.6 Доступ к серверу ограничен паролем, который известен только инженеру по защите информации.

5.7 Коммутаторы, концентраторы, роутеры, точки доступа и прочее активное сетевое оборудование должно располагаться в местах по возможности исключающих свободный доступ.

6. Процедура увольнения сотрудников имеющих доступ к сети

6.1 В случае кадровых перестановок и изменений все ответственные за базы данных переназначаются приказом директора, новым сотрудникам предоставляются логины и пароли для доступа к базам данных.

7. Антивирусная защита

7.1 Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.) Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты. Антивирусная защита организуется на уровне рабочих станций и сервера посредством лицензионного антивирусного программного обеспечения.

7.2 Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

7.3 За своевременное обновление антивирусного программного обеспечения отвечает инженер по защите информации.