Принято на заседании
Совета учреждения
«20» апреля 2020г.
Протокол №3

Утверждаю :
Директор ОГБПОУ «Рязанский железнодорожный колледж»
М.А.Филатов
апреля 2020 г.

# ПОЛОЖЕНИЕ
## о кибербезопасности ОГБПОУ «Рязанский железнодорожный колледж»

### 1.Общие положения

1.1. Настоящее Положение о кибербезопасности (далее - Положение) ОГБПОУ «Рязанский железнодорожный колледж» (далее - Колледж) разработано в соответствии:

- Ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях по защите информации».
- Ст. 9 Закона № 149-ФЗ, п. 5 - информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей подлежит защите в случаях, предусмотренных законом (государственная тайна).
- Гл. 14 Трудового кодекса РФ (далее - ТК РФ) - защита персональных данных работника.
- Федеральным законом от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию".
- Федеральным законом от 27.07.2006 № 152-ФЗ РФ «О персональных данных», обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

В Колледже развернута локально-вычислительная сеть с выходом в интернет, подлежащая информационной защите.

Под безопасностью локально-вычислительной сети Колледжа понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Безопасность системы достигается обеспечением конфиденциальности обрабатываемой информации, а также целостности и доступности компонентов и ресурсов системы.

Безопасность системы обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств, программ, данных и служб с целью обеспечения доступности, целостности и конфиденциальности, связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки выполнения системой определенных функций в строгом соответствии с их запланированным порядком работы.

Систему обеспечения безопасности включает следующие подсистемы:

- компьютерную безопасность;
- безопасность данных;
- безопасное программное обеспечение;
- безопасность коммуникаций.

Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств

компьютера с целью обеспечения доступности, целостности и конфиденциальности, связанных с ним ресурсов.

Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашения.

Безопасное программное обеспечение представляет собой общецелевые и прикладные программы и средства, осуществляющие безопасную обработку данных в системе и безопасно использующие ресурсы системы.

Безопасность коммуникаций обеспечивается посредством аутентификации телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам критичной информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

К объектам информационной безопасности Колледжа 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.

1.2. Настоящее Положение определяет задачи, функции, обязанности, ответственность и права ответственных за информационную безопасность Колледжа.

1.3. Ответственные за информационную безопасность назначаются приказом директора Колледжа.

1.4. Ответственные за информационную безопасность подчиняются директору Колледжа.

1.5. Ответственные за информационную безопасность в своей работе руководствуются настоящим Положением.

1.6. Ответственные за информационную безопасность в пределах своих функциональных обязанностей обеспечивают безопасность информации, обрабатываемой, передаваемой и хранимой при помощи информационных средств Колледжа.

## 2. Основные задачи и функции ответственных за информационную безопасность

2.1. Основными задачами ответственных за информационную безопасность являются:

2.1.1. Организация эксплуатации технических и программных средств защиты информации.

2.1.2. Текущий контроль работы средств и систем защиты информации.

2.1.3. Организация и контроль резервного копирования информации на сервере ЛВС.

2.2 Ответственные за информационную безопасность выполняют следующие основные функции:

2.2.1. Разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.

2.2.2. Обучение персонала и пользователей ПК правилам безопасной обработки информации и правилам работы со средствами защиты информации.

2.2.3. Организация антивирусного контроля носителей информации и файлов электронной почты, поступающих в Колледж.
2.2.4. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.
2.2.5. Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.
2.2.6. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.
2.2.7. Контроль пользования Интернетом.

2.3. Права ответственных лиц за информационную безопасность.
2.3.1.Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения и электронных платежей.
2.3.2. Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.

2.4. Обязанности ответственных лиц за информационную безопасность.
2.4.1 Обеспечение функционирования и поддержания работоспособности средств и систем защиты информации, в пределах, возложенных на них обязанностей.
2.4.2 Немедленное информирование директора Колледжа о выявленных нарушениях и несанкционированных действиях пользователей, в том числе о случаях несанкционированного доступа в Интернет, а также принятие необходимых мер по устранению нарушений.
2.4.3. Принятие мер совместно с программистами по восстановлению работоспособности средств и систем защиты информации.
2.4.4. Проведение инструктажей сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.
2.4.5. Создание и удаление учетных записей пользователей.
2.4.6 Администрирование работы сервера ЛВС, размещение и классифицирование информации на сервере ЛВС.
2.4.7. Установление по согласованию с директором Колледжа критериев доступа пользователей на сервер ЛВС.
2.4.8.Формирование и представление паролей для новых пользователей, администрирование прав пользователей.
2.4.9. Отслеживание работы антивирусных программ, проведение один раз в неделю полной проверки компьютеров на наличие вирусов.
2.4.10. Регулярное выполнение резервного копирования данных на сервере, при необходимости восстановление потерянных или поврежденных данных.
2.4.11. Ведение и учет пользователей «точки доступа к Интернету». В случае необходимости, лимитирование времени работы пользователя в Интернете и объема скачиваемой информации.
2.5.На ответственных за информационную безопасность возлагается персональная ответственность за качество проводимых ими работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными настоящим Положением.

**3.Базы данных.**

3.1. Все процедуры по использованию и обслуживанию базы 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.

3.2.В случае если база данных требует парольной защиты, то ответственный за базу данных руководствуется требованиями раздела 7 «Система аутентификации» настоящего Положения.

**4.Система аутентификации.**

4.1. На клиентских ПК используется WINDOWS XP PROFESSIONAL, WINDOWS 7, WINDOWS 10.
4.2. Для всех пользователей баз данных устанавливаются уникальные пароли.
4.3. Периодичность плановой смены паролей 1 раз в начале учебного года.
4.4. Установить блокировку учетной записи пользователей при неправильном наборе пароля более пяти раз.
4.5. Установить блокировку экрана и клавиатуры при отсутствии активности пользователя на рабочем месте более 30 мин., с последующим вводом пароля для разблокирования ПК.
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 более 1,5 часов.
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 сеть (Интернет, электронная почта) осуществляется через компьютеры с установленными брандмауэром 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 станций к внешним линиям связи производится в локальной вычислительной сети по протоколам Ethernet и WiFi.
5.4. Запрещено подключение к сети WiFi различных мобильных устройств (личных телефонов, планшетов и других гаджетов).

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

6.1. Колледжные серверы размещаются в компьютерных кабинетах.
6.2. Доступ к серверам ограничен паролем, который известен только заведующим кабинетами, ответственному за информационную безопасность, ответственному за информатизацию, инженеру - программисту.
6.3. Коммутаторы, концентраторы, роутеры, точки доступа и прочее активное сетевое оборудование должно располагаться в местах по возможности

исключающих свободный доступ.

**7. Процедура переназначения сотрудников, имеющих доступ к сети.**

7.1.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.

**8.Антивирусная защита**

8.1. 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.

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

8.3. За своевременное обновление антивирусного программного обеспечения отвечает ответственный за кибербезопасность.