Приложение 13
к приказу от 14.02.2022 № 8

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
«ЦЕНТР МОЛОДЕЖНЫХ ИНИЦИАТИВ»
КОРСАКОВСКОГО ГОРОДСКОГО ОКРУГА САХАЛИНСКОЙ ОБЛАСТИ
(МАУ «ЦМИ»)
Адрес: 694020, Сахалинская область, г.Корсаков, ул.Восточная, 29/2,
телефон: 8(42435)4-00-59, e-mail: mbu_cmi2016@mail.ru

УТВЕРЖДАЮ:
и.о. директора МАУ «ЦМИ»
_____ Д.М.Шпачук
Приказ № 8 от 14.02.2022

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
В МУНИЦИПАЛЬНОМ АВТОНОМНОМ УЧРЕЖДЕНИИ
«ЦЕНТР МОЛОДЕЖНЫХ ИНИЦИАТИВ»
КОРСАКОВСКОГО ГОРОДСКОГО ОКРУГА САХАЛИНСКОЙ ОБЛАСТИ

Корсаков
2022

1. Общие положении

Настоящее Положение регламентирует вопросы информационной безопасности в муниципальном автономном учреждении «Центр молодежных инициатив» Корсаковского городского округа Сахалинской области (далее - МАУ «ЦМИ»),

В МАУ «ЦМИ» развернута локально-вычислительная сеть с выходом в интернет, подлежащая информационной защите.

Под безопасностью локально-вычислительной сети МАУ «ЦМИ» 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 ею 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 можно разбить на 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 МАУ «ЦМИ» 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. Системное администрирование и обязанности ответственного за информационную безопасность.

2.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы ответственного за информационную безопасность по обслуживанию компьютерной техники в МАУ «ЦМИ».

2.2. Ответственным за системное администрирование и информационную безопасность в МАУ «ЦМИ» является работник, назначенный приказом директора.

2.3. Для решения задач информационной безопасности ответственный за информационную безопасность должен:

- 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.);
- Обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;
- Обеспечивать мероприятия по антивирусной защите;
- Обеспечивать нормальное функционирование системы резервного копирования.

3. Система аутентификации.

3.1 На всех персональных компьютерах МАУ «ЦМИ» (далее - ПК) используются операционные системы Windows.

3.2 Для пользователей, работающих с персональными данными, устанавливаются уникальные пароли.

3.3 Пользователь не имеет права разглашать сетевые реквизиты (имена и пароли) для доступа к информационным ресурсам, а также хранить их в недоступном месте.

3.4 Обслуживание системы аутентификации осуществляют ответственный за информационную безопасность.

4. Защита по внешним цифровым линиям связи.

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

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

4.3 Подключение рабочих станций к внешним линиям связи производится в локальной вычислительной сети по протоколам Ethernet и WiFi.

4.4 Запрещено подключение различных мобильных устройств (личных телефонов, планшетов и других гаджетов) к сети WiFi.

5. Защита от несанкционированного подключении к ЛВС п размещение активного сетевого оборудования.

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

6. Процедура увольнения работников, имеющих доступ к сети.

В случае кадровых перестановок и изменений новым работникам предоставляются логины и пароли для доступа к базам данных.

7. Антивирусная защита.

7.1 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 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 ответственный за информационную безопасность.