УТВЕРЖДАЮ
И.О.Директора кадетского училища
_____ В.Н.Густов

Политика информационной безопасности Витебского кадетского училища

1. Общие положения

1.1. Настоящая политика информационной безопасности предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса обработки данных в Витебском кадетском училище (далее – училище).

Настоящая Политика регламентирует порядок обеспечения сохранности информации и ее безопасности в училище в осуществлении текущей деятельности.

1.2. Цель и назначение настоящей Политики

Целями настоящей Политики являются:

сохранение конфиденциальности информационных ресурсов;

обеспечение непрерывности доступа к информационным ресурсам училища для поддержки деятельности;

защита целостности деловой информации с целью поддержания возможности училища по оказанию услуг высокого качества и принятию эффективных управленческих решений;

повышение осведомленности работников в области рисков, связанных с информационными ресурсами;

определение степени ответственности и обязанностей работников по обеспечению информационной безопасности в училище.

1.3. Предметом настоящей политики является:

- порядок доступа к конфиденциальной информации;
- физическая безопасность (доступ в помещения);
- разграничение прав доступа;
- работа в глобальной сети Интернет;
- дублирование, резервирование и хранение конфиденциальной информации.

2. Порядок доступа к конфиденциальной информации

2.1. В целях обеспечения защиты информации в училище, устанавливается следующий порядок допуска к работе с конфиденциальными источниками:

- решение о доступе работника к определенному разделу информации принимается руководством.
- инженер-программист (инженер-электроник) обеспечивают защиту отдельных файлов и программ от чтения, удаления, копирования лицами, не допущенными к этому.

Доступ к компьютерной сети осуществляется только с персональным паролем. Пользователь должен держать в тайне свой пароль. Сообщать свой пароль другим лицам, а также пользоваться чужими паролями запрещается.

Категорически запрещается снимать несанкционированные копии с носителей информации, знакомить с содержанием электронной информации лиц, не допущенных к этому.

3. Физическая безопасность

3.1. Все объекты критичные с точки зрения информационной безопасности (все сервера баз данных, основной маршрутизатор, файервол) находятся в отдельном помещении, доступ в которое разрешен только инженеру-программисту, инженеру-электронику.

3.2. Помещение оборудовано охранной и пожарной сигнализациями.

3.3. Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования может находиться в помещении только в присутствии работников, находящихся в помещении в связи с выполнением своих должностных обязанностей.

4. Разграничение прав доступа к программному обеспечению и системам хранения данных

4.1. Для входа в компьютерную сеть училища работник, учащийся должен ввести имя и пароль. Не допускается режим беспарольного (гостевого) доступа.

4.2. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

4.3. В процессе своей работы сотрудникам рекомендуется постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

5. Работа в глобальной сети Интернет

5.1.Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

5.2. Рекомендованные правила:

сотрудникам разрешается использовать сеть Интернет только в служебных целях;

запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, иные материалы с оскорбительными высказываниями по поводу возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

сотрудники не должны использовать сеть Интернет для хранения служебных данных;

работа сотрудников с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации в сеть Интернет;

сотрудники училища перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

5.3. Инженер-программист (инженер-электроник) имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6. Дублирование, резервирование и хранение конфиденциальной информации

6.1. В целях защиты информации от преднамеренного или же непреднамеренного ее уничтожения, фальсификации или разглашения обеспечить резервирование всей информации, имеющей конфиденциальный характер, дублирование информации с использованием различных физических и аппаратных носителей.

Юрисконсульт Ю.Ю.Ярков

Инженер-электроник А.И.Петров