Положение по информационной безопасности

1. Общие положения

Данный локальный акт регламентирует вопросы информационной безопасности в Государственном бюджетном образовательном учреждении средняя общеобразовательная школа №255 с углубленным изучением предметов художественно-эстетического цикла Адмиралтейского района Санкт-Петербурга (далее ГБОУ №255)

В ГБОУ №255 развернута локально-вычислительная сеть с выходом в интернет, подлежащая информационной защите.

Под безопасностью локально-вычислительная сети ГБОУ №255 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 ГБОУ №255 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 ответственного за информационную безопасность по обслуживанию компьютерной техники в ГБОУ №255.
2.2 Для решения задач информационной безопасности ответственный за информационную безопасность должен:

2.2.1 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.);

2.2.2 Обеспечивать функционирование программно-аппартного комплекса защиты по внешним цифровым линиям связи;

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

2.2.4 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.
3.2. Для каждой базы данных включенной в «Реестр баз данных подлежащих информационной защите» приказом директора ГБОУ №255 по представлению Комиссии по информационной безопасности должен назначаться Ответственный за ведение базы данных.
3.3. 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.

3.4. Все изменения «Реестра баз данных подлежащих информационной защите» осуществляется по решению Комиссии по информационной безопасности, состоящей из директора ГБОУ №255, ответственного за информационную безопасность, ответственного за информационную безопасность, ответственного за ведение базы данных.
3.6. 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-ученик, пользователь учитель, администратор с разграничением прав доступа к папкам файлового сервера.
4.3. 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 (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 школьных рабочих станций к внешним линиям связи производится в локальной вычислительной сети по протоколам Ethernet и WiFi.

5.4. Запрещено подключение различных мобильных устройств (личных телефонов, планшетов и других гатжетов) к школьной сети WiFi.

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

6.1. Школьный\е сервер\а размещаются в кабинете информатики при отсутствии специально выделенной серверной.
6.2. Доступ к серверу ограничен паролем, который известен только ответственному за информационную безопасность, ответственному за информатизацию, инженеру.
6.3. Коммутаторы, концентраторы, роутеры, точки доступа и прочее активное сетевое оборудование должно располагаться в местах по возможности исключающих свободный доступ.

7. Процедура увольнения 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 информационную безопасность.

Директор Е.Б.Капитанова

ПРИЛОЖЕНИЕ 1.

Реестр баз данных подлежащих информационной защите

№пп	Наименование базы данных	Ответственный	Режим доступа

ПРИЛОЖЕНИЕ 2.

Состав комиссии по информационной безопасности

В состав Комиссии по информационной безопасности входят:

1. директор ГБОУ №255,
2. ответственный за информатизацию,
3. ответственный за информационную безопасность,
4. ответственные за ведение баз данных.

ПРИЛОЖЕНИЕ 3.

Тезаурус

Конфиденциальность компьютерной информации — это свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы (пользователям, программам, процессам и т. д.).

Целостность компонента (ресурса) системы — свойство компонента (ресурса) быть неизменным (в семантическом смысле) при функционировании системы.

Доступность компонента (ресурса) системы — свойство компонента (ресурса) быть доступным для использования авторизованными субъектами системы в любое время.