МИНИСТЕРСТВО ОБРАЗОВАНИЯ КИРОВСКОЙ ОБЛАСТИ
КОГПОАУ «САВАЛЬСКИЙ ПОЛИТЕХНИКУМ»

Утверждаю
Директор техникума
_____Г.В. Санникова
«___»_____2016 г.

Санникова Галина Владимировна
Подписано цифровой подписью: Санникова Галина Владимировна
Дата: 2021.02.04 12:13:59 +03'00'

ПОЛОЖЕНИЕ О ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КИРОВСКОМ ОБЛАСТНОМ ГОСУДАРСТВЕННОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ АВТОНОМНОМ УЧРЕЖДЕНИИ «САВАЛЬСКИЙ ПОЛИТЕХНИЧЕСКИЙ ТЕХНИКУМ»

Рассмотрено и одобрено на заседании
наблюдательного Совета техникума
Протокол № _ от «___» _____2016 г.

1. Общие положения

КОГПОАУ «Савальский политехникум» – объект, на котором развернута локально-вычислительная сеть, подлежащая информационной защите.

Под безопасностью локально-вычислительная сети техникума 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.

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.

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 техникума относят:

- информационные ресурсы, содержащие сведения, отнесенные к коммерческой тайне, и конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;
- средства и системы информатизации — средства вычислительной и организационной техники, сети и системы, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации, а также их информативные физические поля.

2. О системном администраторе

2.1. Задачи связанные с информационной безопасностью являются прерогативой системного администратора.

2.2. Для решения задач информационной безопасности системный администратор должен:

2.2.1. Следить за соблюдением требований по парольной защите, в том числе осуществлять изменение паролей по разработанному графику;

2.2.2. Обеспечивать функционирование программно-аппаратного 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.

2.3. При числе обслуживаемых машин свыше 40 задачи связанные с информационной безопасностью должны возлагаться на специалиста по информационной безопасности, который осуществляет свою деятельность под непосредственным руководством системного администратора.

3. Базы данных (БД)

3.1. Состав баз данных, подлежащих защите, оформляется приказом директора техникума.

3.2. Для каждой БД приказом директора должен назначаться Администратор базы данных.

3.3. Все процедуры по использованию и обслуживанию базы данных осуществляет Администратор 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. Исключение баз осуществляется приказом директора техникума.
3.5. Предложения по включению или исключению баз данных подаются руководителями структурных подразделений эксплуатирующих базы данных.
3.6. В случае если база данных требует парольной защиты, то Администратор базы руководствуется требованиями главы 4 настоящего документа «Система аутентификации», в которой описаны требования к паролям, их длине, месту хранения, и т.д.
3.7. Подключение и отключение новых пользователей осуществляет Администратор базы данных на основании решения директора.

4. Система аутентификации

4.1. На всех клиентских ПК использовать WINDOWS XP или WINDOWS 7.
4.2. Для всех пользователей устанавливать уникальные пароли длиной не менее 8 знаков.
4.3. Периодичность плановой смены паролей 1 раз в квартал.
4.4. Установить блокировку учетной записи пользователей при неправильном наборе пароля более пяти раз. Вести журнал блокировок учетных записей и их причин.
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.
4.7. Обязать пользователей осуществлять выход из сети, 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 осуществляет системный администратор.
4.10. Базу пользовательских паролей хранить на машинных носителях только в зашифрованном виде.
4.11. Пароли администраторов хранить в запечатанных конвертах, в местах исключающих свободный доступ.

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 одну точку (компьютер) защищенную от несанкционированного доступа извне брэндмауэром и антивирусом.

5.2. Запрещено несанкционированное использование модемов или иных средств доступа с ПК, подключенных к внутренней сети, во внешние сети.
5.3. Время доступа и тип программного обеспечения, посредством которого осуществляется доступ во внешние сети определяется системным администратором.

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

7.1. Для размещения серверов оборудуются специальные серверные комнаты, имеющие два независимых ввода по питанию (~220В), источники бесперебойного питания, систему кондиционирования и оборудованные пожарной и охранной сигнализацией.
7.2. В серверных комнатах не допускается оборудование постоянных рабочих мест для персонала.
7.3. В случае необходимости выполнения каких-либо работ в серверных комнатах посторонним персоналом (электрики, сантехники, уборщики и т.д.) обязательно присутствие системного администратор или его заместители.
7.4. Коммутаторы, концентраторы и прочее активное сетевое оборудование должно располагаться в местах исключающих свободный доступ.
7.5. Магистральные кабели (между отдельными зданиями) не реже одного раза в год осматриваются на предмет отсутствия повреждений, а также, возможных несанкционированных подключений.

8. Договор с пользователями о неразглашении

При заключении трудового договора с сотрудниками специально оговаривается ответственность сотрудника на случай разглашения им информации связанной с функционированием ЛВС техникума. К такой информации относятся имена пользователей, пароли, архитектура сети, виды применяемых методов защиты и т.д. При первичном получении доступа к сетевым ресурсам, пользователи должны проходить вводный инструктаж с регистрацией в специальном журнале и получать на руки памятку (составленную на базе «Положения по информационной безопасности»), содержащую перечень требований по информационной безопасности обязательных для выполнения. Ответственный за инструктаж – системный администратор.

9. Процедура увольнения сотрудников имеющих доступ к сети

9.1. В случае увольнения системного администратора, или администратора какого-либо уровня, после подписания заявления об увольнении немедленно назначается исполняющий обязанности увольняемого сотрудника, который меняет все пароли доступа к ресурсам подконтрольным увольняемому сотруднику. На учетную запись увольняемого администратора устанавливается

ограничение по дате с учетом даты фактического прекращения работы увольняемого.

9.2. В случае увольнения рядового пользователя, после подписания заявления об увольнении секретарь директора уведомляет копией приказа системного администратора о дате фактического прекращения работы увольняемого пользователя. Системный администратор устанавливает ограничения по дате на учетную запись увольняемого сотрудника, по истечении которой учетная запись будет заблокирована, а в дальнейшем уничтожена. Новый сотрудник, принимаемый в последствии на данное рабочее место должен получать НОВУЮ учетную запись, с НОВЫМ именем и паролем.

10. 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 двухуровневой. Верхний уровень антивирусной защиты располагается на коммуникационном сервере техникума, через который осуществляется выход во внешние сети. Нижний уровень располагается на каждом персональном компьютере. Тип применяемого антивирусного программного обеспечения (как серверного, так и пользовательского) определяется системным администратором и является общим для всего техникума. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в неделю. Своевременность обновления антивирусного программного обеспечения обеспечивает системный администратор.