Государственное автономное учреждение дополнительного образования
«Верхнесинячихинская детская школа искусств»

ПОЛОЖЕНИЕ
об информационной безопасности

р.п. Верхняя Синячиха
2020 год

Использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Электронные средства хранения даже более уязвимы, чем бумажные: размещаемые на них данные можно и уничтожить, и скопировать, и незаметно видоизменить.

Число компьютерных преступлений растет – также увеличиваются масштабы компьютерных злоупотреблений. По оценке специалистов США, ущерб от компьютерных преступлений увеличивается на 35 процентов в год. Одной из причин является сумма денег, получаемая в результате преступления: в то время как ущерб от среднего компьютерного преступления составляет 560 тысяч долларов, при ограблении банка – всего лишь 19 тысяч долларов.

По данным Миннесотского университета США, 93% компаний, лишившихся доступа к своим данным на срок более 10 дней, покинули свой бизнес, причем половина из них заявила о своей несостоятельности немедленно.

Число служащих в организации, имеющих доступ к компьютерному оборудованию и информационной технологии, постоянно растет. Доступ к информации больше не ограничивается только узким кругом лиц из верхнего руководства организации. Чем больше людей получает доступ к информационной технологии и компьютерному оборудованию, тем больше возникает возможностей для совершения компьютерных преступлений.

Компьютерным преступником может быть любой.

Типичный компьютерный преступник – это не молодой хакер, использующий телефон и домашний компьютер для получения доступа к большим компьютерам. Типичный компьютерный преступник – это служащий, которому разрешен доступ к системе, нетехническим пользователем которой он является. В США компьютерные преступления, совершенные служащими, составляют 70-80% ежегодного ущерба, связанного с компьютерами.

Среди самых крупных утечек данных в России 2019 года, которые удалось зафиксировать, можно выделить следующие инциденты:

23 сентября 2019 г. специалисты компании по кибербезопасности DeviceLock сообщили Известиям, что с сервера оператора фискальных данных (ОФД) «Дримкас» утекло 76 млн. записей, которые содержали полные реквизиты фискальных чеков, включая порядковые номера, дату и время, ФИО продавца, количество товара, их названия и цены.

1 октября 2019 г. портал об информационной безопасности Comparitech.com совместно с исследователем по кибербезопасности Бобом Дьяченко обнаружили в Интернете 20 млн. налоговых деклараций российских граждан, которые больше года были доступны без пароля на сервере Amazon Elasticsearch. Данные содержали ФИО, адреса, статусы резидентов, номера паспортов, телефонные номера, суммы налогов.

27 февраля 2019 г. портал autonews.ru опубликовал расследование, в котором утверждалось, что за сумму подписки в 750 руб./сутки или 2 500 руб./месяц можно было получить доступ к базе 30 млн. автовладельцев, которые оплачивали парковку в Москве при помощи мобильного приложения Департамента транспорта Москвы или просто по номеру телефона. При заказе отчета можно было получить подробные данные из баз ГИБДД, включая госномера всех когда-либо зарегистрированных на гражданина автомобилей, VIN-номера, номера ПТС и СТС, даты, места и продолжительность стоянки.

1 октября 2019 г. уже упомянутым ранее Бобом Дьяченко в сотрудничестве со специалистами портала Comparitech.com была обнаружена база с 20 млн. налоговых деклараций граждан России за период с 2009 по 2016 год, которая была доступна без пароля на сервере Amazon Web Services Elasticsearch. Записи включали в себя ФИО,

адреса, статусы резидентов, номера паспортов, телефонные номера, идентификационные номера налогоплательщиков, имена работодателей и суммы налогов.

7 октября 2019 г. Коммерсанту стало известно, что данные 9 млн. абонентов широкополосного доступа в Интернет от «Билайн» выложили в сеть. Сотрудники издательства, у которых подключен или был когда-то подключен интернет от «Билайна», нашли в базе свое полное ФИО, адрес, мобильный и домашний телефоны.

1. Общие положения

1.1. Положение об информационной безопасности (далее по тексту – Положение) Государственного автономного учреждения дополнительного образования Свердловской области «Верхнесинячихинская ДШИ» (далее по тексту – ГАУДОСО «Верхнесинячихинская ДШИ») определяет организацию, осуществление и контроль мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам ГАУДОСО «Верхнесинячихинская ДШИ».

1.2. Положение разработано в соответствии с Федеральным законом от 29.12.2012 года № 273-ФЗ «Об образовании в Российской Федерации», Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 7 октября 2017 года № 1235 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства образования и науки Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства образования и науки Российской Федерации, и формы паспорта безопасности этих объектов (территорий)», с целью осуществления мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам ГАУДОСО «Верхнесинячихинская ДШИ».

1.3. Для обеспечения информационной безопасности ГАУДОСО «Верхнесинячихинская ДШИ», приказом заведующего ГАУДОСО «Верхнесинячихинская ДШИ» назначаются ответственные лица за обеспечение информационной безопасности ГАУДОСО «Верхнесинячихинская ДШИ», которые в своей работе руководствуются данным Положением.

1.4. Положение принимается решением Общего собрания работников ГАУДОСО «Верхнесинячихинская ДШИ», с учетом мнения профсоюзного комитета первичной профсоюзной организации ГАУДОСО «Верхнесинячихинская ДШИ», утверждается приказом заведующего ГАУДОСО «Верхнесинячихинская ДШИ». Изменения и дополнения в настоящее Положение вносятся решением Общего собрания работников ГАУДОСО «Верхнесинячихинская ДШИ», с учетом мнения профсоюзного комитета первичной профсоюзной организации ГАУДОСО «Верхнесинячихинская ДШИ», утверждаются приказом заведующего ГАУДОСО «Верхнесинячихинская ДШИ».

1.5. Срок действия данного Положения не ограничен. Положение действует до принятия нового.

2. Цели и задачи информационной безопасности

2.1. Цель: осуществление мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам ГАУДОСО «Верхнесинячихинская ДШИ».

2.2. Основными задачами обеспечения информационной безопасности являются:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;

– реализация права на доступ к информации;

– организация эксплуатации технических и программных средств защиты информации.

2.3. Текущий контроль работы средств и систем защиты информации.

2.4. Организация и контроль резервного копирования информации.

3. Ответственные лица за обеспечение информационной безопасности

3.1. Ответственные лица за обеспечение информационной безопасности (далее по тексту – ответственные лица) в пределах своих функциональных обязанностей обеспечивают безопасность информации обрабатываемой, передаваемой и хранимой при помощи информационных средств в ГАУДОСО «Верхнесинячихинская ДШИ».

3.2. Ответственные лица за информационную безопасность выполняют следующие основные функции:

– разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете;

– обучение работников-пользователей персональных компьютеров (далее по тексту - ПК) правилам безопасной обработки информации и правилам работы со средствами защиты информации;

– организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в ГАУДОСО «Верхнесинячихинская ДШИ»;

– текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации;

– контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём;

– контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК;

– контроль пользования Интернетом.

4. Обязанности ответственных лиц за обеспечение информационной безопасности

4.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах, возложенных на них обязанностей. Немедленно докладывать заведующему ГАУДОСО «Верхнесинячихинская ДШИ» о выявленных нарушениях и несанкционированных действиях работников-пользователей ПК, а также принимать необходимые меры по устранению нарушений.

4.2. Совместно с программистами обслуживающих ГАУДОСО «Верхнесинячихинская ДШИ» организаций (при наличии контракта, договора и т.д.), принимать меры по восстановлению работоспособности средств и систем защиты информации.

4.3. Проводить инструктаж работников-пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.

4.4. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.

4.5. Контролировать регулярное резервное копирование данных (не реже чем один раз в неделю) всеми пользователями ПК, иметь возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

4.6. Предотвращать несанкционированный доступ к информации и (или) передачи ее лицам, не имеющим права на доступ к информации.

4.7. Своевременно выявлять факты несанкционированного доступа к информации.

4.8. Предупреждать возможности неблагоприятных последствий нарушения порядка доступа к информации.

4.9. Не допускать воздействия на технические средства обработки информации, в результате которого нарушается их функционирование.

4.10. Постоянно контролировать обеспечение высокого уровня защищенности информации в ГАУДОСО «Верхнесинячихинская ДШИ».

5. Права ответственных лиц за обеспечение информационной безопасности

5.1. Требовать от работников-пользователей ПК безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения.

5.2. Готовить предложения по совершенствованию системы информационной безопасности ГАУДОСО «Верхнесинячихинская ДШИ».

6. Ответственность ответственных лиц за информационную безопасность

6.1. На ответственных лиц за информационную безопасность ГАУДОСО «Верхнесинячихинская ДШИ» возлагается персональная ответственность за качество проводимых ими работ по обеспечению информационной безопасности ГАУДОСО «Верхнесинячихинская ДШИ», защиты информации в соответствии с функциональными обязанностями, определёнными настоящим Положением.