МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«Проект политики информационной безопасности школы»**

Студент:

Борисов Антон Андреевич

Вариант 1

Преподаватель:

Блинова Евгения Александровна

Минск 2021

**Обоснование актуальности, цели и задачи разработки политики информационной безопасности в организации**

Политика Школы в области информационной предусматривает принятие необходимых мер в целях защиты ресурсов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Школе.

Информация существует в различных формах: на бумажном носителе, в электронном виде при хранении на носителе, передается по почте или с использованием электронных устройств, передаваться устно в процессе общения. Информация должна быть защищена независимо от ее формы и способа ее распространения, передачи и хранения.

Информационная безопасность — это защита информации от различных угроз, призванная обеспечить непрерывность бизнес-процессов, минимизировать риски и обеспечить возможности служебной деятельности.

Главные цели Школы не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник Школы. На лиц, работающих в Школе по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

Целью Политики является создание условий, позволяющих предотвратить или минимизировать ущерб, который может быть нанесен в результате несанкционированного доступа, хищения служебной информации или нанесения ущерба техническим средствам обработки, хранения и передачи защищаемой информации.

Под защитой информационных ресурсов следует понимать:

* сохранение конфиденциальности информационных ресурсов;
* обеспечение непрерывности доступа к информационным ресурсам Школы в сферах его деятельности;
* защита целостности служебной информации с целью поддержания возможности Школы по оказанию услуг высокого качества и принятию эффективных управленческих решений;
* повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Школы;
* определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Школе.

Руководители структурных подразделений Школы должны обеспечить регулярный контроль за соблюдением положений настоящей Политики, организовать периодические проверки соблюдения информационной безопасности с последующим представлением ежегодного отчета по результатам указанной проверки Руководству.

**Объекты защиты**

К объектам информационной безопасности в учереждении относятся:

-информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

-информацию, защита которой предусмотрена законодательными актами Республики Беларусь, в т. ч. персональные данные;

-средства и системы информатизации. программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

-информация по финансово-экономической деятельности образовательного учреждения;

-персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

-научные достижения школы;

-время работников сотрудников;

-другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

**Основные угрозы и их источники. Оценка рисков.**

Угроза безопасности - потенциальное нарушение безопасности, любое обстоятельство или событие, которое может явиться причиной нанесения ущерба предприятию в целом.

Источники угроз по отношению к инфраструктуре школы могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются:

* Сотрудники школы;
* Программное обеспечение;
* Аппаратные средства.

К информационным угрозам относятся:

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* противозаконный сбор и использование информации;
* использование информационного оружия.

К программным угрозам относятся:

* поиск «дыр» в OC, firewall, Proxy-серверах;компьютерные вирусы и вредоносные программы.

К физическим угрозам относятся:

* уничтожение или разрушение средств обработки информации и связи.

Условная численная шкала для оценки ущерба школы от несанкционированного доступа(НСД) представлена в таблице 1

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации принесет ничтожный моральный и финансовый ущерб школе |
| 1 | Ущерб от атаки есть, но он незначителен |
| 2 | Ущерб от атаки значителен, но не создаёт угрозы для школы |
| 3 | Ущерб значителен, есть угроза закрытия школы |
| 4 | Школа прекращает своё существование |

Таблица 1 — Условная численная шкала для оценки ущерба школы от НСД

Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам представлена в таблице 2

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

Таблица 2 — Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

Таблица рисков представлена ниже

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (ущерб \* вероятность) |
| Кража паспортных данных | 2 | 0,2 | 0,4 |
| Кража информации о плане работы школы | 1 | 0,1 | 0,2 |
| Попытки несанкционированного администрирования баз данных | 2 | 0,1 | 0,2 |
| Запуск игровых программ | 0 | 0,5 | 0 |
| Получение информации о уровнях дохода | 2 | 0,2 | 0,4 |
| Установка вирусных программ и троянских коней | 2 | 0,3 | 0,6 |
| Несанкционированная откачка из Интернета нелицензионного софта и установка его на рабочие станции | 1 | 0,4 | 0,4 |
| Попытки проникновения в системы бухгалтерского учета | 2 | 0,1 | 0,2 |
| Кража информации научных работ | 1 | 0,1 | 0,1 |
| Поиск «дыр» в OC, firewall, Proxy-серверах | 1 | 0,3 | 0,3 |
| Попытки несанкционированного удаленного администрирования ОС | 2 | 0,2 | 0,4 |

Таблица 3 — Таблица рисков для объектов информационной системы школы

Таким образом можно сделать вывод, что наиболее опасными видами атаки являются установка вирусных программ и троянских коней и попытки несанкционированной откачки из Интернета нелицензионного софта и установка его на рабочие станции, а наиболее частыми атаками является установка игровых программ.

**Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов**

Для обеспечения информационной безопасности в школе требуется проведение следующих первоочередных мероприятий:

Защита интеллектуальной собственности образовательной организации;

Защита компьютеров, локальных сетей и сети подключения к системе Интернета;

Организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся образовательной организации;

Учет всех носителей конфиденциальной информации.

Использование сети Интернет работниками школы допускается только в целях исполнения ими своих должностных обязанностей и в целях образовательного процесса, использование сети Интернет обучающимися допускается только для обеспечения образовательного процесса.

Использование сети Интернет в образовательной организации в личных целях работниками и обучающимися не допускается.

В целях своевременного выявления угроз, связанных с получением доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, , иную информацию, распространение которой запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, в образовательной организации проводится периодический контроль состояния системы обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет, в том числе контроль функционирования технических средств контентной фильтрации и антивирусной защиты.

Обучающиеся в случае выявления наличия доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, незамедлительно информирует педагогического работника, ведущего занятие, или иного ответственного работника школы.

Педагогический работник, ведущий занятие, иной ответственный работник школы  обязан осуществлять постоянный контроль использования технических средств, применяемых при организации доступа к сети Интернет (программных, программно-аппаратных), в том числе контроль функционирования технических средств контентной фильтрации, а также контроль доступа обучающихся к ресурсам сети Интернет.  
       При получении информации от обучающихся о получении доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, или в случае самостоятельного выявления наличия доступа к таким ресурсам сети Интернет, незамедлительно принимать меры, направленные на прекращение и ограничение доступа обучающихся к такой информации, а также информировать об инциденте работника образовательной организации, ответственного за организацию доступа к сети Интернет.

При организации доступа и использовании сети Интернет в школе работники школы несут персональную ответственность в соответствии действующим законодательством.

Обучающиеся и их родители (законные представители) несут ответственность за неправомерное использование сети Интернет в порядке, установленном в образовательной организации, и в соответствии с действующим законодательством.

Каждый  сотрудник, получивший в пользование персональный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

Все   компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей Политики ИБ являются собственностью организации.

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация школы.

Сотрудникам   запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор локальной вычислительной сети (ЛВС).

Все   компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима «Экранной заставки».

Должен обеспечиваться узкий круг лиц, имеющих доступ к информационным данным;

Обучения пользованием компьютера с целью предотвращения случайной отправки информации чужому получателю;

Установка видеокамер в школе;

**Выводы:**

Даже казалось бы такое безобидное и спокойное место как школа, может быть целью наблюдения злоумышленников. Использование школы как место отсидки после преступления. Получения паспортных данных с целью банковских махинаций. Информация о уровне дохода родителей с целью будущего шантажа под предлогом ребёнка. Информация о времени работы сотрудников с целью ограбления их жилья или их рабочих мест и т.д

Поэтому очень важно предусмотреть как можно больше возможных угроз места наблюдения с целью предотвращения злых умыслов и спокойной жизни граждан.