Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Проект политики информационной безопасности**

для школы

Выполнил: Белицкий В.Д.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

**Введение**

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Для построения системы защиты информации необходимо определить границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности (система защиты информации) должна строиться именно в этих границах.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Существуют различные подходы к оценке рисков. Выбор под хода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Разработанная и утвержденная документация должна включать в себя следующие разделы:

* перечисление объектов, в отношении которых устанавливается режим информационной безопасности, их ранжирование по значимости и требуемой степени защиты;
* описания технологий, применяемых для обеспечения сохранности информации;
* перечень действующих и потенциальных угроз информационной безопасности, описание степени их серьезности и реализуемости;
* описание внешних и внутренних субъектов, которые могут стать источниками потенциальной угрозы;
* описание понятия инцидента информационной безопасности, процедур уведомления о его возникновении;
* описание применяемых организационных мер, действий сотрудников организации по обеспечению информационной безопасности;
* описание выбранной политики защиты от вирусных атак, программ-вредителей, возможных действий хакеров;
* описание системы резервного копирования важных данных, ее периодичности, моделей хранения – на дисках, на посторонних серверах;

**Цели и задачи политики информационной безопасности**

Целью политики является регламентирование единых подходов и требований по обеспечению информационной безопасности сотрудниками образовательного учреждения, а также государственными органами и организациями, иными юридическими лицами и индивидуальными предпринимателями в рамках оказания им услуг образовательное учреждением.

Достижение указанной цели предполагает решение следующих задач:

* реализация требований законодательства государства в части информационной безопасности информационных систем и мер контроля их защищенности;
* определение ответственности субъектов информационных отношений по обеспечению и соблюдению требований политики, в том числе с использованием программных, программно-аппаратных средств технической и криптографической защиты информации, а также посредством принятия соответствующих внутренних нормативных и организационно-методических документов информационной безопасности образовательного учреждения;
* своевременное выявление и оценка причин, условий и характера угроз информационной безопасности и дальнейшее прогнозирование развития событий на основе мониторинга инцидентов информационной безопасности;
* планирование и контроль эффективности использования защитных мер и средств защиты информации, создание механизма оперативного реагирования на угрозы информационной безопасности;

Основной целью информационной безопасности обеспечение конфиденциальности и целостности доверенных учебному образования документов, в которые входят:

1. документы, содержащие информацию о учащихся
2. документы бухгалтерского учета
3. сведения об успеваемости учеников

**Объекты защиты**

Объектами защиты с точки зрения информационной безопасности являются:

* Информационный процесс профессиональной деятельности.
* Информационные активы образовательного учреждения.
* База данных образовательного учреждения.
* Вся собранная информация о учащихся и работниках.

Субъектами защиты с точки зрения информационной безопасности являются:

* Учащиеся школы
* Родители учеников
* Сотрудники

Структура образовательного учреждения – это форма организации его внутренних элементов: подразделений, управлений и служб**.**

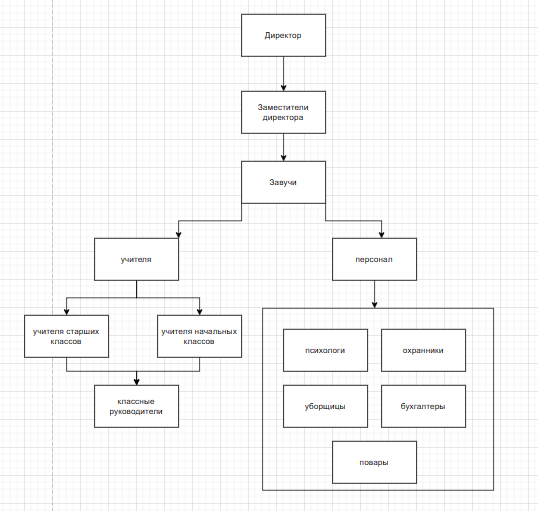
****

Рисунок 1 –Структура образовательного учреждения

Среди внутренних аспектов проживания школы особенно важными оказываются:

* Основные направления деятельности: хранение информации об учащихся, выставление оценок, предоставление доступа только лицам, прошедшим процесс аутентификации;
* Масштаб деятельности образовательного учреждения: республика, города, населенные пункты;

Высшее руководство (дирекция) — в его компетенцию входит принятие основополагающих решений по поводу целевых установок и образовательной политики образовательного учреждения, подбор и расстановка кад­ров, руководство нижестоящими управленческими подразделениями.

Среднее руководство (учителя) осуществляет управление отдельными сферами образовательной деятельности, регулирование процесса проживания, руководство подчиненными служащими, подготовку принятия решений для дирекции.

Низшее руководство (психологи, воспитатели) следят за поведением учащихся.

Основным структурными информационными объектами образовательного учреждения являются - базы данных образовательного учреждения, хранящая информацию о учащихся, их картах: номер в журнале, идентификационные характеристики; личные данные клиента: адрес, семейное положение, место проживания, дата рождения

**Основные угрозы и их источники.**

В Зависимости от источника угрозы их классифицируют по следующим параметрам:

* Естественные.
* Искусственные.
* Внешние.
* Внутренние.
* Преднамеренные.
* Непреднамеренные.

**К естественным** угрозам информационной безопасности относятся:

* Перебои с электроэнергией.
* Сбои в работе базы данных.
* Короткое замыкание.

**Искусственные:**

* Механическое повреждение оборудования.
* Халатное отношение персонала школы к оборудованию.
* DDOS атаки на сервера школы.
* MITM атаки.
* Прослушивание трафика.

**Внешние угрозы:**

* Утечки конфиденциальной информации через сотрудников.
* Шантаж сотрудников.
* Вирусы в электронных письмах.

**Внутренние:**

* Кража документов из школы.
* Несанкционированный доступ и прослушивание внутреннего вай-фая.

**Преднамеренные:**

* Программы-вымогатели.
* Задняя-дверь.
* Все виды хакерских атак

**Непреднамеренные:**

* Ошибки в программном обеспечении.
* Непреднамеренное разглашение данных о учениках.

**Вредоносное ПО** — это аббревиатура от «вредоносное программное обеспечение», которое включает в себя вирусы, червей, троянов, программ-шпионов и программ-вымогателей и является наиболее распространенным типом кибератака. Вредоносное ПО проникает в систему, как правило, через ссылку на ненадежном веб-сайте или по электронной почте, или через загрузку нежелательного программного обеспечения. Он развертывается в целевой системе, собирает конфиденциальные данные, манипулирует и блокирует доступ к сетевым компонентам, а также может уничтожить данные или полностью отключить систему.

**Социальная инженерия** включает в себя обман пользователей, чтобы они предоставили точку входа для вредоносных программ. Жертва предоставляет конфиденциальную информацию или невольно устанавливает вредоносное ПО на свое устройство, потому что злоумышленник выдает себя за законного деятеля.

**Оценка рисков**

Ценность информационных ресурсов образовательного учреждения характеризуется возможным вредом системе образования, а также понижением её репутационных характеристик. Особой ценностью обладают информационных объекты, содержащие информацию о учащихся образовательного учреждения, о их оценках и любой информации об учащихся. Не меньшей ценностью аттестаты, табели, журналы, их бумажные и электронные копии.

Значимость определённых угроз зависит от вреда, которые они могут нанести информационным системам образования в целом. Примеры угроз:

* нарушение целостность информации, хранящейся на серверах учреждения;
* получения доступа к информации третьими лицами;
* обнародование секретной или конфиденциальной информации;
* несанкционированный доступ к помещениям, содержащим ценные бумаги и документы;
* различные стихийные бедствия, приводящие к нарушению целостности здания школы и уничтожения информационных объектов и т.д.

Минимальным требованиям к режиму информационной безопасности соответствует базовый уровень. Обычной областью использования этого уровня являются типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т.д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности осуществления угроз и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

Оценка эффективности существующих или планируемых средств защиты основывается на глубоком анализе истории неблагоприятных для информационной системы образовательного учреждения ситуаций: возникновение серверных атак, конфликтных ситуаций с учащимися, возникших на основе нарушения целостности информации и получения третьими лицами доступа к конфиденциальной информации и т.д.

Чтобы определить вероятность выполнения одного из критических сценариев развития, угрожающих целостности информационной системе, ситуаций необходимо оценить привлекательность информационного ресурса как показателя при рассмотрении угрозы от умышленного воздействия со стороны человека:

* аттестаты, документы – высокая ценность;
* справочная информация, база данных обучающихся – средняя ценность;
* записки от родителей, неофициальные документы – средняя, низкая ценность.

Таблица 1. Оценка рисков

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск |
| DDOS-атака | 3 | 0,4 | 1,2 |
| Фишинг | 4 | 0,3 | 1,2 |
| Шантаж | 2 | 0,1 | 0,2 |
| Программные сбои | 3 | 0,3 | 0,9 |
| Повреждение оборудования | 2 | 0,1 | 0,2 |
| MITM-атака | 5 | 0,5 | 2,5 |
| Проникновение в архив | 5 | 0,1 | 0,5 |
| Backdoor | 4 | 0,1 | 0,4 |
| Брутфорс | 1 | 0,1 | 0,1 |
| Руткит | 5 | 0,5 | 2,5 |
| Флуд | 1 | 0,1 | 0,1 |
| Подкуп сотрудников | 2 | 0,2 | 0,4 |
| Итог |  |  | 10,2 |

**Разработка мер защиты**

На основании политики безопасности строится программа безопасности, которая реализуется на процедурном и программно-техническом уровнях.

**Процедурный уровень**

Можно выделить следующие группы процедурных мер:

* управление персоналом:

1. для каждой должности существуют квалификационные требования по информационной безопасности. Таким образом, необходимо ограничить доступ и предоставить достаточно высокий уровень доступа определённым работникам образовательного учреждения. Работники образовательного учреждения, которым предоставлен высший уровень доступа к аттестатам учащихся, документам, базам данных и серверным должны быть должным образом проинструктированы о политике информационной безопасности образовательного учреждения и быть готовы реагировать на внештатные ситуации в соответсвии с распорядком;
2. весь рабочий персонал должен быть проинструктирован о возможных угрозах информационной безопасности образовательного учреждения;
3. каждый работник должен изучить меры безопасности теоретически и на практике;
4. отдельным работникам доступ к важным бумагам и информационным объектам должен быть ограничен;
5. физическая защита:
6. установка охранных и охранно-пожарных систем в здании образовательного учреждения;
7. установка средств охранного телевидения: камеры, экраны наблюдения, зеркальные щиты и т.д.;
8. установка охранного освещения;
9. установка, где присутствует необходимость, ограждений и физической изоляции;
10. установка запирающих устройств на дверные проёмы и двери;
11. установка систем контроля доступа: карты доступа, средства опознавания по отпечаткам пальцев, голосу, почерку, геометрии рук;
12. установка радиолучевых, радиоволновых и инфракрасных защитных систем: антенн, глушителей и т.д.
13. поддержание работоспособности:
14. проведение своевременных ревизий защитного оборудования образовательного учреждения;
15. ежедневный контроль исправности защитного оборудования;
16. реагирование на нарушения режима безопасности:
17. необходимо назначить несколько рабочих лиц, отвественных за безопасность информационной системы образовательного учреждения;
18. разделение локальных сетей образовательного учреждения на сегменты и своевременной их отключение;
19. активизация всех защитных систем образовательного учреждения и блокировка доступа ко всем объектам информационной системы образовательного учреждения;
20. обеспечение информационной системы образовательного учреждения избыточными мерами резервного копирования, хранения копий информации и представления информации в разных видах;
21. заключение соглашений с поставщиками информационных услуг по защите информации;
22. проверка и практическая реализация стратегии восстановительных работ;
23. определение средств штатной проживания образовательного учреждения в случае критической ситуации и прорабатывание с персоналом образовательного учреждения сценариев развития внештатных ситуаций.

**Программно-технический уровень**

Основой программно-технического уровняявляются следующие механизмы безопасности:

1. установка средств идентификации/аутентификации учеников (паролей, средств двухфакторной аутентификацией и т.д.);
2. предоставление необходимости подтвердить свою личность в случае подозрительной деятельности пользователя;
3. предоставление необходимости смены пароля или иных средств идентификации/аутентификации в случае длительного их использования или подозрительной деятельности пользователя;
4. предоставление работникам образовательного учреждения средств контроля доступа за деятельностью учеников;
5. ограничение доступа к отдельным составляющим информационной системы для отдельных учеников;
6. полное ограничение и предоставление необходимости в подтверждении прав доступа для учеников, проявляющих подозрительную активность;
7. контроль за действиями пользователя во время пользования информационной системой;
8. постоянный аудит работоспособности защитных устройств и систем отдельных информационных объектов;
9. проведение анализа защищённости объектов и процедур по проверке отказоустойчивости защитных систем;
10. криптография:
11. обеспечение надёжных систем шифрования данных;
12. постоянная разработка и модификация алгоритмов шифрования;
13. установка средств экранирования информационных каналов;
14. мониторинг информационных систем на факт наличия источников утечки информации;
15. установка защитного антивирусного программного обеспечения на объекты информационной системы образовательного учреждения.
16. структуризация элементов информационной системы;
17. автоматизация процессов информационной системы;
18. обеспечение модульности архитектуры информационной системы;
19. ориентация на простоту решений при разработке архитектуры информационной системы.

**Выводы**

Правильное составление содержания политики информационной безопасности является важным аспектом построения успешной и защищённой организации. Политика информационной безопасности организации содержит основные и базовые инструкции по установке, регулированию и контролю защитных средств.

Политика информационной безопасности помогает основательно подготовить учреждение к непредвиденным ситуациям и быстро решить возникшую проблему. Также, она содержит инструкции по информационной безопасности для рабочего персонала образовательного учреждения и может использоваться как пособие для консультации работников образовательного учреждения по вопросам данной сферы.

Политика информационной безопасности является одним из звеньев в последовательном ряде решений информационной безопасности, указанное обстоятельство гарантирует должностным лицам образовательного учреждения, что система информационной безопасности, построенная в соответствии с концепцией, будет управляемой, экономически обоснованной и соответствующей требованиям бизнеса.