МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра программной инженерии

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программное обеспечение информационных технологий (программирование интернет-приложений)

**ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ:**

по дисциплине «Информационная безопасность»

Исполнитель

студент (к3 курса группы 6 Розель Станислав Александрович

(Ф.И.О.)

Минск 2024

**1. Обоснование актуальности, цели и задачи разработки ПИБ в организации**

В условиях цифровизации образования и увеличения объемов обрабатываемой информации университеты становятся объектами повышенного внимания злоумышленников. Утечки данных, кибератаки, несанкционированный доступ к информации могут привести к серьезным последствиям, включая финансовые потери, репутационные риски и нарушение образовательного процесса. Разработка ПИБ позволяет минимизировать риски и обеспечить защиту информационных ресурсов.

Целями защиты информации является защита университет от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИС, а также минимизация рисков ИБ.

Основными задачами университет в части обеспечения безопасности информации в ИС являются:

* + реализация требований законодательства Республики Беларусь в части информационной безопасности ИС и мер контроля их защищенности;
  + определение ответственности участников, которые работают с информацией, за выполнение требований по защите данных. Это включает использование программного и аппаратного обеспечения для защиты информации, применение методов криптографической защиты, а также создание внутренних правил и документов, связанных с информационной безопасностью университета;
  + минимизация ущерба, который может быть нанесен университет из-за нарушений ИБ;
  + разграничение доступа пользователей к ИС;
  + обеспечение аутентификации пользователей;
  + обеспечение регистрации действий пользователей ИС в системных журналах и организация контроля этих действий путем анализа содержимого журналов;
  + обеспечение защиты от несанкционированной модификации используемого в ИС программного обеспечения, а также защиты ИС от внедрения несанкционированных программ, включая вредоносное ПО;
  + обеспечение резервирования и архивирования информационных ресурсов;
  + обеспечение криптографической защиты информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, при ее передаче посредством сетей электросвязи общего пользования;
  + своевременное выявление и оценка причин, условий и характера угроз ИБ, дальнейшее прогнозирование и профилактика развития событий ИБ на основе мониторинга инцидентов ИБ;
  + выявление, предупреждение и пресечение возможности противоправной и иной деятельности работников и обучающихся университет;
  + реализация программ по осведомленности и обучению работников университет о возможных факторах рисков ИБ и мерах противодействия.

#### 2. Объекты защиты.

#### 2.1. Структура университета

Университет как организация состоит из множества подразделений, каждое из которых обрабатывает различные типы информации. Основные структурные элементы:

* **Администрация университета:**
  1. Ректорат: управление университетом, стратегическое планирование.
  2. Деканаты: управление факультетами, учебный процесс.
  3. Отделы: кадровый, бухгалтерия, юридический, IT-отдел, отдел информационной безопасности.
* **Факультеты и кафедры:**
  1. Факультеты: организационные единицы, отвечающие за образовательные программы.
  2. Кафедры: учебно-научные подразделения, занимающиеся преподаванием и исследованиями.
* **Учебные и научные подразделения:**
  1. Библиотеки.
  2. Лаборатории.
  3. Учебные классы и аудитории.
  4. Компьютерные классы.
* **Техническая инфраструктура:**
  1. IT-отдел: обслуживание серверов, сетей, рабочих станций.
  2. Отдел информационной безопасности: обеспечение защиты данных.
* **Вспомогательные подразделения:**
  1. Бухгалтерия: финансовая информация.
  2. Кадровый отдел: персональные данные сотрудников.
  3. Юридический отдел: правовая информация.

#### 2.2. Объекты защиты

Объекты защиты — это информационные и технические ресурсы, которые требуют защиты от угроз. К ним относятся:

* **Информационные ресурсы:**
  1. Персональные данные студентов и сотрудников (ФИО, паспортные данные, адреса, номера телефонов).
  2. Учебные материалы: лекции, методические пособия, электронные курсы.
  3. Научные исследования: данные экспериментов, публикации, патенты.
  4. Финансовая информация: бюджеты, зарплаты, договоры.
  5. Административная информация: приказы, распоряжения, отчеты.
* **Технические ресурсы:**
  1. Серверы и базы данных.
  2. Сетевые устройства (маршрутизаторы, коммутаторы).
  3. Рабочие станции и мобильные устройства.
  4. Системы хранения данных (СХД).
* **Программное обеспечение:**
  1. Лицензионное ПО: операционные системы, офисные приложения.
  2. Специализированное ПО: для управления учебным процессом и научными исследованиями.

#### 2.3. Субъекты информационных отношений

Субъекты — это лица, которые взаимодействуют с информационными ресурсами университета:

* **Сотрудники университета:**
  1. Преподаватели и научные сотрудники.
  2. Административный персонал (ректорат, деканаты, отделы).
  3. IT-специалисты и сотрудники отдела информационной безопасности.
* **Студенты:**
  1. Обучающиеся на всех формах обучения (очная, заочная, дистанционная).
* **Внешние партнеры:**
  1. Поставщики услуг (интернет-провайдеры, облачные сервисы).
  2. Подрядчики (разработчики ПО, консультанты по ИБ).
  3. Государственные органы (министерства, налоговые службы).

#### 3. Основные угрозы и их источники

**Естественные угрозы:**

* Стихийные бедствия (пожары, наводнения).
* Сбои электропитания.
* Воздействие мощных электромагнитных и электрических помех (промышленных и природных).
* Сбои и отказы в аппаратуре сбора, обработки и передачи информации;

**Искусственные угрозы:**

* **Преднамеренные:**
  1. Кибератаки (вирусы, фишинг, DDoS-атаки).
  2. Хищение данных.
  3. Саботаж со стороны недовольных сотрудников.
* **Непреднамеренные:**
  1. Ошибки персонала.
  2. Неосторожное обращение с данными.

**Источники угроз:**

* Внешние: хакеры, конкуренты, злоумышленники, ранее уволенные сотрудники.
* Внутренние: сотрудники, студенты, технические сбои, технический персонал, программисты, системные администраторы, администраторы ИБ.

#### 4. Оценка угроз, рисков и уязвимостей.

#### 4.1 Оценка значимости угроз

|  |  |  |  |
| --- | --- | --- | --- |
| **Описание атаки/угрозы** | **Ущерб (0-5)** | **Вероятность (0-0,5)** | **Риск (Ущерб × Вероятность)** |
| Вирусная атака (шифровальщики, трояны) | 3 | 0,3 | 0,9 |
| Несанкционированный доступ к учебным материалам | 3 | 0,3 | 0,9 |
| Фишинг (кража учетных данных) | 3 | 0,3 | 0,9 |
| Неосторожное обращение с данными сотрудниками | 2 | 0,4 | 0,8 |
| Копирование данных с серверов | 3 | 0,2 | 0,6 |
| Несанкционированный доступ к Wi-Fi | 2 | 0,3 | 0,6 |
| Атака на систему управления обучением (LMS) | 3 | 0,2 | 0,6 |
| Утечка персональных данных студентов | 5 | 0,1 | 0,5 |
| Атака на базу данных студентов | 5 | 0,1 | 0,5 |
| DDoS-атака на сайт университета | 2 | 0,2 | 0,4 |
| Кража научных исследований | 4 | 0,1 | 0,4 |
| Спам | 1 | 0,4 | 0,4 |
| Потеря данных из-за сбоя оборудования | 4 | 0,1 | 0,4 |
| Подделка документов (дипломов, справок) | 4 | 0,1 | 0,4 |
| Утечка финансовой информации | 4 | 0,1 | 0,4 |
| **Итого** |  |  | **8,8** |

#### 5. Меры, методы и средства обеспечения защиты

**Политика ИБ:**

* Утверждение правил работы с информацией.
* Регламент доступа к данным.
* План реагирования на инциденты.

**Программа обеспечения безопасности:**

* **Организационные меры:**
  1. Назначение ответственных за ИБ.
  2. Регулярный аудит системы защиты.
  3. Распределенны роли
  4. Созданы следующие ИС:
     1. ИС «Студент»
     2. ИС «Абитуриент»
     3. ИС «Преподователь»
     4. **ИС «Система дистанционного обучения университета»**
     5. **ИС «Бухгалтерия»**
* **Технические меры:**
  1. Установка антивирусов и межсетевых экранов.
  2. Шифрование данных.
  3. Резервное копирование.
* **Обучение:**
  1. Проведение тренингов для сотрудников и студентов.
  2. Информирование о новых угрозах.

#### 6. Ответственность

В соответствии с законодательством Республики Беларусь, несанкционированный доступ к информационным системам, а также их взлом, являются уголовно наказуемыми действиями. Основные статьи Уголовного кодекса Республики Беларусь (УК РБ) [1], касающиеся таких преступлений:

* Статья 354. Несанкционированный доступ к компьютерной информации:
  1. Наказание: штраф, исправительные работы, арест, ограничение свободы или лишение свободы сроком до 2 лет.
  2. Если действия совершены повторно, группой лиц, либо нанесли значительный ущерб, наказание может быть увеличено до 5 лет лишения свободы.
* Статья 352. Несанкционированное завладение компьютерной информацией:
  1. Наказание: лишение свободы до 3 лет.
  2. Если действия связаны с крупным ущербом или совершены повторно, наказание увеличивается до 7 лет лишения свободы.
* Статья 353. Создание, использование или распространение вредоносных программ:
  1. Наказание: лишение свободы до 5 лет.
  2. Если действия повлекли тяжкие последствия, срок лишения свободы может составить до 10 лет.
* Статья 354-1. Нарушение правил защиты компьютерной информации:
  1. Наказание: штраф или арест до 3 месяцев.
  2. Если нарушение повлекло ущерб, наказание может составить до 2 лет лишения свободы.
* Статья 214. Хищение имущества путем использования компьютерной техники:
  1. Наказание: лишение свободы до 4 лет.
  2. При особо крупных размерах ущерба — до 12 лет лишения свободы с конфискацией имущества.

#### 7. Выводы и предложения

Разработка и внедрение ПИБ в университете является необходимым шагом для защиты информационных ресурсов и обеспечения устойчивости образовательного процесса. Для повышения эффективности системы защиты рекомендуется:

* Регулярно обновлять программное обеспечение.
* Внедрять новые технологии защиты (например, двухфакторную аутентификацию).
* Проводить тестирование на проникновение.
* Создать центр мониторинга киберугроз.

Политика ИБ должна быть динамичной и адаптироваться к изменяющимся условиям и новым угрозам.

Список используемых источников

1. Уголовный кодекс Республики Беларусь. [Электронный ресурс] / StrongLoop, Inc. – Режим доступа: https://pravo.by/document/?guid=3871&p0=hk9900275. – Дата доступа: 21.02.2025.