Государственное образовательное учреждение

«Белорусский государственный технологический университет»

Отчет

*по лабораторной работе №3*

ТЕМА ЗАНЯТИЯ: РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БИЗНЕС-КОМПАНИИ

|  |  |
| --- | --- |
|  | **Исполнитель:**  Студента (-ка) группы 2  Специальность\_\_\_\_ИСиТ\_\_\_  Гулевич Никита Максимович  (Ф.И.О.) |
|  | **Преподаватель**:  Ржеутская Н. В. |

Минск, 2025

**Цель**: разработать проект политики информационной безопасности бизнес-компании.

Ответы на контрольные вопросы:

1. Что такое политика безопасности?

Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Политика безопасности должна включать в себя анализ возможных угроз и выбор мер противодействия.

1. Чем отличаются пассивные и активные методы защиты информации от утечки по техническим каналам?

Метки безопасности используются для реализации принудительного управления доступом к субъектам и объектам. Метка субъекта описывает его благонадежность, метка объекта – степень «закрытости» содержащейся в нем информации. Согласно «Оранжевой книге», метки безопасности состоят из двух частей – уровня секретности и списка категорий.

Уровни секретности, поддерживаемые системой, образуют упорядоченное множество, которое может выглядеть, например, так:

− совершенно секретно;

− секретно;

− конфиденциально;

− несекретно.

1. Какие работы производятся по обеспечению режима информационной безопасности?

Работы по обеспечению режима информационной безопасности:

– определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания;

– оценка рисков;

– выбор контрмер, обеспечивающих режим информационной безопасности;

– управление рисками;

– аудит системы управления информационной безопасностью;

– выработка политики безопасности.

Этап 1. Выбор национальных и международных руководящих документов и стандартов в области информационной безопасности и формулирование на их базе основных требований и положений политики информационной безопасности компании, включая: – управление доступом к средствам вычислительной техники (СВТ), программам и данным, а также антивирусную защиту; – вопросы резервного копирования; – проведение ремонтных и восстановительных работ; – информирование об инцидентах в области информационной безопасности и пр.

Этап 2. Выработка подходов к управлению информационными рисками и принятие решения о выборе уровня защищенности компьютерных информационных систем (КИС). Уровень защищенности в соответствии с зарубежными стандартами может быть минимальным (базовым) либо повышенным. Этим уровням защищенности соответствует минимальный (базовый) или полный вариант анализа информационных рисков.

Этап 3. Структуризация контрмер по защите информации по следующим основным уровням: административному, процедурному, программно-техническому.

Этап 4. Установление порядка сертификации и аккредитации КИС на соответствие стандартам в сфере информационной безопасности. Назначение периодичности проведения совещаний по тематике информационной безопасности на уровне руководства, в том числе периодического пересмотра положений политики информационной безопасности, а также порядка обучения всех категорий пользователей информационной системы в области информационной безопасности. Известно, что выработка политики безопасности организации – наименее формализованный этап. Однако в последнее время именно здесь сосредоточены усилия многих специалистов по защите информации.

Этап 5. Определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания. На этом этапе определяются границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности строится именно в этих границах.

1. По характеру проводимых действий как разделяются все методы защиты информации?

**Разделение устройств на многоуровневые и одноуровневые**

Существует разделение устройств на многоуровневые и одноуровневые. На многоуровневых устройствах может храниться информация разного уровня секретности. Зная уровень устройства, система может решить, допустимо ли записывать на него информацию с определенной меткой.

**Принудительное управление доступом**

Принудительное управление доступом основано на сопоставлении меток безопасности субъекта и объекта. Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен – читать можно только то, что положено. Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен.

Принудительное управление доступом реализовано во многих вариантах операционных систем и СУБД, отличающихся повышенными мерами безопасности. В реальной жизни произвольное и принудительное управление доступом сочетается в рамках одной системы, что позволяет использовать сильные стороны обоих подходов.

**Цель подотчетности**

Цель подотчетности – в каждый момент времени знать, кто работает в системе и что он делает. Средства подотчетности делятся на три категории:

* Идентификация и аутентификация;
* Предоставление надежного пути;
* Анализ регистрационной информации (аудит).

Каждый пользователь, прежде чем получить право совершать какие-либо действия в системе, должен идентифицировать себя. В свою очередь система должна проверить подлинность личности пользователя, т. е. что он является именно тем, за кого себя выдает. Идентификация и аутентификация – первый и важнейший программно-технический рубеж информационной безопасности. Если не составляет проблемы получить доступ к системе под любым именем, то другие механизмы безопасности, например управление доступом, очевидно, теряют смысл.

Надежный путь связывает пользователя непосредственно с надежной вычислительной базой, минуя другие, потенциально опасные, компоненты системы. Цель предоставления надежного пути – дать пользователю возможность убедиться в подлинности обслуживающей его системы.

1. Что является основой программно-технического уровня для обеспечения безопасности?

Основой программно-технического уровня являются следующие механизмы безопасности:

− идентификация и аутентификация пользователей;

− управление доступом;

− протоколирование и аудит;

− криптография;

− экранирование;

− обеспечение высокой доступности и т. д.

**ВАРИАНТ 7**

**Политика Информационной Безопасности Библиотеки**

Политика информационной безопасности (ИБ) библиотеки определяет правила и процедуры, направленные на защиту информационных ресурсов, обеспечение их целостности, конфиденциальности и доступности. Эта политика распространяется на всех сотрудников, пользователей и партнеров библиотеки.

Цели и Задачи

* Обеспечение защиты информации от несанкционированного доступа, утечек и уничтожения.
* Минимизация рисков, связанных с информационной безопасностью.
* Обеспечение соответствия требованиям законодательства и стандартов в области ИБ.
* Повышение осведомленности сотрудников о вопросах информационной безопасности.

Область Применения

Политика ИБ распространяется на все информационные системы, базы данных, сети, программное и аппаратное обеспечение, а также на всех сотрудников и пользователей библиотеки.

Основные Принципы

1. Конфиденциальность: Информация должна быть доступна только авторизованным пользователям.
2. Целостность: Информация должна быть защищена от несанкционированных изменений.
3. Доступность: Информация должна быть доступна для авторизованных пользователей в любое время.

Принудительное управление доступом обеспечивает соблюдение политики безопасности на системном уровне:

* Системы библиотеки настроены таким образом, чтобы предотвращать несанкционированный доступ к данным.
* Все действия пользователей контролируются и протоколируются.

**Безопасность повторного использования объектов**

Библиотека обеспечивает безопасность повторного использования объектов, таких как книги, компьютеры и другие ресурсы:

* Все объекты проверяются на наличие вредоносного ПО перед повторным использованием.
* Данные пользователей удаляются с объектов после их использования.

**Произвольное управление доступом**

Произвольное управление доступом позволяет ограничивать доступ к объектам на основе учета личности субъекта или группы, в которую субъект входит. В библиотеке это реализуется следующим образом:

* Владелец объекта (например, книги или базы данных) может по своему усмотрению предоставлять или отбирать права доступа у других пользователей.
* Доступ к конфиденциальной информации предоставляется только авторизованным лицам.

**Матрица доступа**

Произвольное управление доступом (DAC) позволяет библиотекарям и администраторам определять, какие пользователи или группы пользователей могут получить доступ к библиотечным ресурсам (книгам, электронным базам данных, компьютерам) и какие действия они могут выполнять. Текущее состояние прав доступа описывается матрицей, в которой:

* **Строки** представляют пользователей или группы пользователей.
* **Столбцы** представляют библиотечные ресурсы.
* **Клетки** на пересечении строк и столбцов содержат способы доступа, допустимые для пользователя по отношению к ресурсу (например, чтение, запись, выполнение, передача прав).

**Пример матрицы доступа**

| Пользователи / Ресурсы | Книга 1 | Электронная база данных | Компьютер |
| --- | --- | --- | --- |
| Пользователь А | Чтение | Запись | Выполнение |
| Пользователь Б | Запись | - | Чтение |
| Группа В | - | Чтение | Выполнение |

В данном примере Пользователь А имеет право на чтение Книги 1, запись в Электронную базу данных и выполнение операций на Компьютере. Пользователь Б может записывать в Книгу 1 и читать на Компьютере, а Группа В может читать Электронную базу данных и выполнять операции на Компьютере.

**Безопасность повторного использования объектов**

Безопасность повторного использования объектов в библиотеке предотвращает случайное или преднамеренное извлечение конфиденциальной информации из "мусора". Это включает:

* **Очистку оперативной памяти**: Удаление данных из буферов, таких как образы экрана и расшифрованные пароли, после их использования.
* **Очистку дисковых блоков**: Удаление данных с дисков и носителей перед их повторным использованием.
* **Безопасность повторного использования субъектов**: При увольнении сотрудника необходимо не только лишить его возможности входа в систему, но и запретить доступ ко всем ресурсам, чтобы новый сотрудник не мог получить ранее использовавшийся идентификатор и связанные с ним права.

**Метки безопасности**

Метки безопасности используются для реализации принудительного управления доступом (MAC), обеспечивая дополнительный уровень защиты информации в библиотеке. Метки состоят из двух частей:

1. **Уровень секретности**: Определяет степень конфиденциальности информации. Уровни секретности образуют упорядоченное множество, например:
   * Совершенно секретно
   * Секретно
   * Конфиденциально
   * Несекретно
2. **Список категорий**: Описывает предметную область, к которой относятся данные. Категории позволяют разделить информацию по отсекам, предотвращая доступ пользователей к "чужим" категориям, даже если их уровень благонадежности высок.

**Пример использования меток безопасности**

* **Пользователь**: Сотрудник с меткой "Секретно" и категорией "История".
* **Ресурс**: Книга с меткой "Конфиденциально" и категорией "История".

В этом примере сотрудник может получить доступ к книге, так как его уровень секретности выше, чем у книги, и категория совпадает. Если бы категория книги была другой (например, "Медицина"), доступ был бы запрещен, несмотря на более высокий уровень секретности сотрудника.

**Метки безопасности и их целостность**

**Обеспечение целостности меток**

Целостность меток безопасности является ключевым аспектом политики безопасности библиотеки. Для этого необходимо:

* **Полное покрытие меток**: Все субъекты (пользователи) и объекты (ресурсы) должны быть помечены. Не должно быть непомеченных элементов.
* **Сохранение меток при операциях**: При любых операциях с данными метки должны оставаться корректными. Например, печатный документ должен содержать заголовок с текстовым или графическим представлением метки безопасности.

**Многоуровневые и одноуровневые устройства**

Библиотека использует как многоуровневые, так и одноуровневые устройства:

* **Многоуровневые устройства**: Могут хранить информацию разного уровня секретности. Система определяет, допустимо ли записывать на устройство информацию с определенной меткой, зная уровень устройства.
* **Одноуровневые устройства**: Хранят информацию только одного уровня секретности.

**Принудительное управление доступом**

Принудительное управление доступом (MAC) основано на сопоставлении меток безопасности субъектов и объектов. Основные принципы:

* **Доминирование меток**: Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, и все категории объекта присутствуют в метке субъекта.
* **Запрет на понижение уровня секретности**: При любых операциях уровень секретности информации не должен понижаться. Повышение уровня секретности допустимо.

**Пример использования меток безопасности**

* **Субъект**: Библиотекарь с меткой "Секретно" и категориями "История" и "Литература".
* **Объект**: Документ с меткой "Конфиденциально" и категорией "История".

Библиотекарь может получить доступ к документу, так как его уровень секретности выше, и категория совпадает. Если бы категория документа была другой (например, "Медицина"), доступ был бы запрещен.

**Средства подотчетности**

Цель подотчетности – в любой момент времени знать, кто работает в системе и что он делает. Средства подотчетности делятся на три категории:

1. **Идентификация и аутентификация**:
   * Каждый пользователь должен идентифицировать себя перед выполнением действий в системе.
   * Система проверяет подлинность личности пользователя, чтобы убедиться, что он является тем, за кого себя выдает.
2. **Предоставление надежного пути**:
   * Все действия пользователей должны выполняться через защищенные каналы связи, чтобы предотвратить перехват данных.
3. **Анализ регистрационной информации (аудит)**:
   * Ведение протоколов всех действий пользователей.
   * Регулярный аудит протоколов для выявления и предотвращения нарушений.

**Идентификация и аутентификация**

Идентификация и аутентификация являются первым и важнейшим рубежом информационной безопасности. Если доступ к системе может быть получен под любым именем, то другие механизмы безопасности, такие как управление доступом, теряют свою эффективность.

**Основные принципы**

* **Идентификация**: Каждый пользователь должен идентифицировать себя перед выполнением действий в системе. Это может быть реализовано через ввод логина или использование уникального идентификатора.
* **Аутентификация**: Система должна проверять подлинность личности пользователя. Это может включать ввод пароля, использование биометрических данных или других методов проверки.

**Пример реализации**

* **Пользователь**: Библиотекарь вводит свой логин и пароль для доступа к системе управления библиотекой.
* **Система**: Проверяет введенные данные и предоставляет доступ только в случае успешной аутентификации.

**Надежный путь**

Надежный путь связывает пользователя непосредственно с надежной вычислительной базой, минуя потенциально опасные компоненты системы. Цель предоставления надежного пути – дать пользователю возможность убедиться в подлинности обслуживающей его системы.

**Реализация надежного пути**

* **Неинтеллектуальные терминалы**: Использование зарезервированной управляющей последовательности для обеспечения надежного пути.
* **Интеллектуальные терминалы и ПК**: Обеспечение надежного пути становится сложной задачей и требует использования дополнительных мер безопасности, таких как шифрование данных и проверка целостности.

**Аудит и протоколирование**

Аудит и протоколирование являются важными компонентами политики безопасности, позволяющими следить за действиями пользователей и реконструировать прошедшие события.

**Основные события для аудита**

* **Вход и выход из системы**: Фиксация успешных и неуспешных попыток входа.
* **Обращение к удаленной системе**: Мониторинг доступа к внешним ресурсам.
* **Операции с файлами**: Отслеживание действий, таких как открытие, закрытие, переименование и удаление файлов.
* **Смена привилегий**: Контроль изменений в режиме доступа или уровне благонадежности пользователя.

**Цели аудита**

* **Профилактика нарушений**: Знание о том, что действия фиксируются, может предотвратить попытки нарушения безопасности.
* **Реконструкция событий**: Возможность восстановления последовательности действий для расследования инцидентов.

**Гарантированность**

Гарантированность – это мера уверенности в том, что выбранный набор средств для реализации политики безопасности эффективен, а каждое средство выполняет свою роль правильно.

**Виды гарантированности**

* **Операционная гарантированность**: Обеспечение правильной работы всех компонентов системы в процессе эксплуатации.
* **Технологическая гарантированность**: Использование проверенных технологий и методов для защиты информации.

**Пример реализации**

* **Регулярное тестирование**: Проведение тестов для проверки работы системы безопасности.
* **Аудит кода**: Проверка программного кода на наличие уязвимостей.

**Архитектура системы**

Архитектура системы должна быть спроектирована таким образом, чтобы обеспечить выполнение избранной политики безопасности. Это включает:

* **Деление функций по уровням привилегированности**: Контроль обмена информацией между уровнями и минимизация привилегий для каждого компонента.
* **Защита процессов**: Обеспечение независимости процессов и предотвращение их взаимного влияния.
* **Средства управления доступом**: Наличие механизмов для контроля доступа к ресурсам.
* **Структурированность системы**: Выделение надежной вычислительной базы и обеспечение ее компактности.

**Целостность системы**

Целостность системы подразумевает корректную работу всех аппаратных и программных компонентов. Это достигается за счет:

* **Периодической проверки целостности**: Использование аппаратных и программных средств для регулярной проверки состояния системы.
* **Поддержание целостности меток безопасности**: Обеспечение корректности меток при любых операциях с данными.

**Надежное администрирование**

Надежное администрирование предполагает выделение трех ролей:

* **Системный администратор**: Отвечает за техническое обслуживание системы.
* **Системный оператор**: Выполняет текущие операции и мониторинг.
* **Администратор безопасности**: Обеспечивает соблюдение политики безопасности и реагирует на инциденты.

**Надежное восстановление после сбоев**

Надежное восстановление включает подготовку к сбоям и непосредственно восстановление:

* **Подготовка к сбоям**: Регулярное резервное копирование данных, разработка планов действий в экстренных случаях и поддержание запаса резервных компонентов.
* **Восстановление**: Перезагрузка системы и выполнение ремонтных или административных процедур для восстановления работоспособности.

**Технологическая гарантированность**

Технологическая гарантированность охватывает весь жизненный цикл системы, включая проектирование, реализацию, тестирование, продажу и сопровождение.

**Тестирование**

Тестирование должно показать, что защитные механизмы функционируют в соответствии с их описанием и что не существует способов обхода защиты. Это включает:

* **Функциональное тестирование**: Проверка работы всех компонентов системы.
* **Тестирование безопасности**: Поиск уязвимостей и проверка устойчивости к атакам.

**Документация**

Документация является необходимым условием гарантированной надежности системы. В комплект документации должны входить:

* **Руководство пользователя по средствам безопасности**: Инструкции для пользователей по обеспечению безопасности.
* **Руководство администратора по средствам безопасности**: Инструкции для администраторов по управлению безопасностью.
* **Тестовая документация**: Описание проведенных тестов и их результатов.
* **Описание архитектуры**: Подробное описание архитектуры системы.
* **Политика безопасности**: Письменное изложение политики безопасности организации.

**Обеспечение режима информационной безопасности**

Для обеспечения режима информационной безопасности необходимо выполнить следующие работы:

* **Определение границ системы управления информационной безопасностью**: Установление четких границ системы и целей ее создания.
* **Оценка рисков**: Идентификация потенциальных угроз и оценка их вероятности и воздействия.
* **Выбор контрмер**: Разработка мер по снижению рисков и обеспечению безопасности.
* **Управление рисками**: Постоянный мониторинг и обновление мер безопасности в ответ на изменения угроз.

**Этапы разработки политики безопасности**

**Этап 1: Выбор стандартов и формулирование требований**

На этом этапе выбираются национальные и международные стандарты в области информационной безопасности, которые будут использоваться для формулирования основных требований и положений политики безопасности библиотеки. Это включает:

* **Управление доступом**: Определение правил доступа к средствам вычислительной техники, программам и данным.
* **Антивирусная защита**: Внедрение мер по защите от вредоносного ПО.
* **Резервное копирование**: Разработка процедур для регулярного резервного копирования данных.
* **Ремонтные и восстановительные работы**: Определение порядка проведения ремонтных работ и восстановления данных после сбоев.
* **Информирование об инцидентах**: Установление процедур для своевременного информирования о происшествиях в области информационной безопасности.

**Этап 2: Управление информационными рисками**

На этом этапе определяются подходы к управлению информационными рисками и выбирается уровень защищенности компьютерных информационных систем (КИС). Уровень защищенности может быть минимальным (базовым) или повышенным, в зависимости от результатов анализа рисков.

**Этап 3: Структуризация контрмер**

Контрмеры по защите информации структурируются по следующим уровням:

* **Административный уровень**: Меры, предпринимаемые руководством библиотеки, такие как разработка политики безопасности и управление рисками.
* **Процедурный уровень**: Внедрение процедур и инструкций для обеспечения безопасности.
* **Программно-технический уровень**: Использование технических средств для защиты информации.

**Этап 4: Сертификация и аккредитация**

На этом этапе устанавливается порядок сертификации и аккредитации КИС на соответствие стандартам в области информационной безопасности. Также определяется периодичность проведения совещаний по вопросам информационной безопасности и обучения пользователей.

**Этап 5: Определение границ системы управления информационной безопасностью**

На этом этапе определяются границы системы, для которой должен быть обеспечен режим информационной безопасности. Это позволяет сосредоточить усилия на защите наиболее критичных ресурсов и данных.

**Аудит системы управления информационной безопасностью**

Аудит системы управления информационной безопасностью включает в себя регулярную проверку и оценку эффективности мер безопасности. Основные задачи аудита:

* **Проверка соответствия стандартам**: Оценка соответствия системы установленным стандартам и требованиям.
* **Выявление уязвимостей**: Поиск и устранение уязвимостей в системе.
* **Анализ инцидентов**: Изучение происшествий в области информационной безопасности и разработка мер по их предотвращению.
* **Обучение пользователей**: Обучение сотрудников библиотеки основам информационной безопасности и правилам работы с ресурсами.

Описание границ системы управления информационной безопасностью

Структура организации

Библиотека обладает определенной структурой, включающей различные отделы и подразделения, такие как абонемент, читальный зал, электронный ресурсный центр и административный отдел. Внедрение автоматизированной системы обработки информации может потребовать изменений в существующей структуре для обеспечения эффективного управления информационной безопасностью.

Размещение средств вычислительной техники и инфраструктуры

Средства вычислительной техники (СВТ) и поддерживающая инфраструктура размещаются в специально оборудованных помещениях с контролируемым доступом. Иерархия СВТ включает серверы, рабочие станции, сетевое оборудование и периферийные устройства.

Ресурсы, подлежащие защите

Ресурсы информационной системы библиотеки, подлежащие защите, включают:

* Средства вычислительной техники: Серверы, рабочие станции, сетевое оборудование.
* Данные: Электронные каталоги, базы данных, цифровые копии книг и документов.
* Программное обеспечение: Системное и прикладное ПО, используемое для управления библиотечными процессами.

Для оценки ценности ресурсов используется система критериев, включающая степень важности данных для функционирования библиотеки и потенциальные последствия их утраты или повреждения.

Технология обработки информации и решаемые задачи

Основные задачи, решаемые с помощью информационной системы библиотеки, включают:

* Управление каталогами и фондами.
* Обработка запросов пользователей.
* Обеспечение доступа к электронным ресурсам.

Для каждой задачи строятся модели обработки информации, учитывающие используемые ресурсы и их взаимодействие.

Оценка рисков

Процесс оценки рисков включает несколько этапов:

1. Идентификация ресурсов: Определение ресурсов, подлежащих защите, и оценка их количественных показателей.
2. Оценка угроз: Анализ потенциальных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ.
3. Оценка уязвимостей: Выявление уязвимостей в системе, которые могут быть использованы для реализации угроз.
4. Оценка существующих средств защиты: Анализ текущих мер безопасности и их эффективности.
5. Оценка рисков: Определение вероятности реализации угроз и потенциального ущерба для ресурсов.

Меры по обеспечению информационной безопасности

Базовый уровень защиты

Базовый уровень защиты включает стандартные меры, направленные на нейтрализацию наиболее вероятных угроз:

* Антивирусная защита.
* Регулярное резервное копирование данных.
* Контроль доступа к ресурсам.
* Обучение сотрудников основам информационной безопасности.

Дополнительные меры защиты

Для ресурсов, нарушение безопасности которых может привести к серьезным последствиям, разрабатываются дополнительные меры защиты:

* Внедрение систем обнаружения вторжений.
* Использование шифрования для защиты конфиденциальной информации.
* Регулярный аудит системы безопасности.

**Оценка рисков**

Цель оценки рисков заключается в определении характеристик рисков для информационной системы и ее ресурсов. Это позволяет выбрать необходимые средства управления информационной безопасностью. При оценке рисков учитываются следующие факторы:

* Ценность ресурсов: Определение значимости ресурсов для функционирования библиотеки.
* Оценка значимости угроз: Анализ потенциальных угроз и их воздействия на ресурсы.
* Эффективность средств защиты: Оценка существующих и планируемых мер безопасности.

Показатели рисков

Показатели рисков могут быть определены несколькими способами:

* Количественные показатели: Например, стоимость утраты данных или финансовые потери от сбоев.
* Качественные показатели: Использование оценок, таких как "умеренный" или "чрезвычайно опасный".
* Комбинированные показатели: Сочетание количественных и качественных методов для более точной оценки.

Вероятность реализации угроз

Вероятность реализации угроз определяется следующими факторами:

* Привлекательность ресурса: Насколько ресурс привлекателен для злоумышленников.
* Возможность получения дохода: Может ли ресурс быть использован для получения прибыли.
* Технические возможности угрозы: Наличие технических средств для реализации угрозы.
* Степень легкости использования уязвимости: Насколько легко можно воспользоваться уязвимостью при существующих мерах защиты.

Процедурные меры безопасности

Процедурные меры безопасности включают действия, выполняемые людьми для обеспечения информационной безопасности. Основные группы процедурных мер:

* Управление персоналом: Включает квалификационные требования по информационной безопасности, обучение сотрудников и наличие разделов, касающихся безопасности, в должностных инструкциях.
* Физическая защита: Обеспечение контроля доступа к помещениям и оборудованию.
* Поддержание работоспособности: Создание инфраструктуры, обеспечивающей необходимый уровень работоспособности системы.
* Реагирование на нарушения: Регламентация действий при обнаружении инцидентов безопасности.
* Планирование восстановительных работ: Разработка планов действий на случай аварий, включая использование резервных площадок.

Программно-технические меры безопасности

Основные механизмы программно-технического уровня включают:

* Идентификация и аутентификация: Проверка подлинности пользователей при доступе к системе.
* Управление доступом: Контроль прав доступа к ресурсам.
* Протоколирование и аудит: Ведение журналов событий и их анализ для выявления инцидентов.
* Криптография: Использование шифрования для защиты данных.
* Экранирование: Защита от несанкционированного доступа к информации.
* Обеспечение высокой доступности: Меры по поддержанию непрерывной работы системы.

УГРОЗЫ

1. Угрозы физической и логической целостности

1.1 уничтожение данных или инфраструктуры

Меры защиты:

* резервное копирование данных: регулярное создание резервных копий и их хранение в защищенных местах
* физическая защита серверного оборудования: использование защищенных серверных помещений с контролем доступа
* системы аварийного питания: использование ИБП (источников бесперебойного питания) и резервных генераторов
* мониторинг и контроль доступа: установка видеонаблюдения, датчиков движения, сигнализации

1.2 модификация данных

Меры защиты:

* контроль целостности данных: использование хеширования (SHA-256, MD5) для проверки неизменности информации
* журналирование действий пользователей: логирование всех изменений с возможностью аудита
* разграничение прав доступа: запрет редактирования данных для неавторизованных пользователей
* использование систем обнаружения атак (IDS/IPS): мониторинг трафика и автоматическое блокирование подозрительной активности

1.3 повреждение данных или оборудования

Меры защиты:

* физическая защита оборудования: установка противопожарных систем, климат-контроля, антивандальных корпусов
* программные меры: использование антивирусов, средств защиты от вредоносного ПО
* изоляция критически важных систем: хранение особо важных данных на защищенных сегментах сети

2. Угрозы конфиденциальности

2.1 несанкционированный доступ к персональным данным граждан

Меры защиты:

* шифрование данных: использование алгоритмов AES-256 для защиты информации
* политика минимизации доступа: доступ только тем сотрудникам, кому это действительно необходимо
* многофакторная аутентификация (MFA): защита учетных записей пользователей
* мониторинг и аудит доступа: логирование всех попыток доступа к персональным данным

2.2 утечка данных через сотрудников (инсайдерская угроза)

Меры защиты:

* обучение персонала: периодическое обучение сотрудников основам ИБ
* система DLP (Data Loss Prevention): автоматический контроль передачи конфиденциальных данных
* разграничение прав доступа: доступ к информации только по должностным обязанностям
* юридическая ответственность: включение пунктов о конфиденциальности в трудовые договоры

3. Угрозы доступности

3.1 блокировка работы информационных систем (DDoS-атаки)

Меры защиты:

* фильтрация трафика: использование специальных сервисов защиты от DDoS (Cloudflare, Imperva)
* распределение нагрузки: использование балансировщиков трафика и облачных решений
* резервные серверы: использование резервных мощностей для обеспечения работы в случае атаки

3.2 сбой оборудования

Меры защиты:

* мониторинг состояния серверов: использование систем автоматического мониторинга (Zabbix, Nagios)
* запасные компоненты: хранение резервных жестких дисков, блоков питания, серверов
* обновление оборудования: регулярная замена устаревшего оборудования

4. Угрозы прав собственности

4.1 кража данных или незаконное использование информации

Меры защиты:

* авторизация и аутентификация: использование сложных паролей и многофакторной аутентификации
* контроль действий пользователей: логирование всех операций и мониторинг подозрительной активности
* правовое регулирование: разработка политики использования данных, юридические соглашения

5. Случайные угрозы (в т.ч. стихийные)

5.1 случайные угрозы (ошибки, сбои, аварии)

Меры защиты:

* регулярное резервное копирование: ежедневное или еженедельное создание резервных копий
* автоматизированные системы контроля: обнаружение ошибок и предупреждение о возможных сбоях
* разделение прав пользователей: исключение возможности случайного удаления данных

5.2 преднамеренные угрозы (взломы, диверсии)

Меры защиты:

* защита от кибератак: использование брандмауэров и антивирусов
* обучение сотрудников методам защиты: проведение киберучений
* физическая безопасность: охрана серверных комнат, ограничение доступа

6. Обобщение угроз по источникам

6.1 человеческий фактор (сотрудники, злоумышленники)

Меры защиты:

* регулярные тренинги: обучение персонала кибербезопасности
* система выявления аномальной активности: автоматический мониторинг действий пользователей
* ограничение доступа: разграничение прав и двухфакторная аутентификация

6.2 технические устройства (сбои, несовместимость систем)

Меры защиты:

* регулярное обновление оборудования и ПО
* использование систем мониторинга неисправностей
* резервирование оборудования и сетевых каналов

6.3 ошибки в ПО, уязвимости в коде

Меры защиты:

* использование проверенных программных решений
* регулярное обновление ПО и установка патчей безопасности
* код-ревью и тестирование перед внедрением новых функций

6.4 внешняя среда (пожары, стихийные бедствия, электромагнитные помехи)

Меры защиты:

* размещение серверов в безопасных центрах обработки данных
* использование противопожарных систем и систем аварийного электропитания
* создание резервных копий данных в удаленных дата-центрах

**Заключение**

Политика безопасности библиотеки включает в себя комплекс мер, направленных на оценку рисков, реализацию процедурных и программно-технических мер безопасности. Эти меры позволяют защитить информацию и ресурсы от различных угроз, обеспечить надежную работу информационной системы и минимизировать последствия инцидентов.

**Список использованных источников**

1. Концепция национальной безопасности РБ, Указ №575
2. [Национальный исследовательский университет «МЭИ»](https://studfile.net/mei/) [Методы и Средства Защиты Информации](https://studfile.net/mei/miszi/folder:44331/#5868802): Подготовительный практикум.

https://studfile.net/preview/5868802/

1. Ржеутская Н. В., Нистюк О. А., Уласевич Н. И. Основы защиты информации: лабораторный практикум. Минск: Учреждение образования «Белорусский государственный технологический университет», 2024.