Федеральное государственное образовательное бюджетное   
учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЕТ   
Практическая работа №9**

**По теме**

**“Разработка требований безопасности информационной системы”**

**Дисциплина /Профессиональный модуль:** Проектирование и дизайн информационных систем

**Студент: Карабут Борис**

**Группа: 3ИСИП-521**

|  |  |  |
| --- | --- | --- |
|  |  | **Преподаватель:** |
|  |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_/Абзалимов Р. Р/ |
|  |  | **Дата выполнения:** |
|  |  | 19.12.2023 г. |

Москва   
2023

**Цель:**

Получение навыков разработки требований безопасности информационной системы.

**Задание № 1:**

Цель системы защиты информации - это обеспечение безопасности и конфиденциальности данных. Задачи системы включают в себя идентификацию и аутентификацию пользователей, контроль доступа к информации, обнаружение и предотвращение несанкционированного доступа, а также резервное копирование и восстановление данных.

Задачи защиты информации включают:

* Идентификацию и аутентификацию пользователей для контроля доступа к информации.
* Шифрование данных для защиты их конфиденциальности.
* Резервное копирование и восстановление данных для обеспечения их доступности.
* Мониторинг и обнаружение несанкционированной активности для предотвращения вторжений.
* Обучение и осведомление пользователей о правилах и процедурах безопасности информации

**Задание № 2:**

Основными факторами, влияющими на информационную безопасность предприятия, являются:

* Тип и масштаб информационной системы: чем больше система и
* сложнее ее структура, тем больше ресурсов требуется для ее защиты.
* Уровень конфиденциальности данных: если данные являются конфиденциальными, то система защиты должна быть более строгой.
* Количество и квалификация пользователей: с увеличением числа пользователей сложнее контролировать их действия.
* Внешние угрозы: система защиты должна учитывать возможные

угрозы от злоумышленников извне.

* Выбор и настройка технических средств защиты: необходимо учитывать требования к безопасности и особенности информационной системы при выборе и настройке технических средств защиты.
* Правовые и нормативные требования: система защиты информации должна соответствовать законодательству и стандартам в области информационной безопасности.
* Экономические ограничения: организация системы защиты информации требует определенных затрат, поэтому необходимо учитывать экономические возможности организации.
* Человеческий фактор: сотрудники организации могут быть источником угроз безопасности, поэтому важно проводить обучение и контролировать соблюдение правил информационной безопасности.

**Задание № 3:**

Дестабилизирующее воздействие -негативное воздействие на компьютерную систему, реализуемое использованием реализации угрозы ИБ, в результате чего происходит нарушение конфиденциальности информации, её уничтожение, блокирование, модификация.

Существует множество дестабилизирующих факторов:

* Количественная недостаточность системы защиты — совокупность факторов, не позволяющих перекрыть известное множество каналов утечки информации путем применения существующих средств защиты, которые по своим характеристикам могут полностью обеспечить безопасность информации;
* Качественная недостаточность системы защиты — совокупность факторов, не позволяющих перекрыть известное множество каналов утечки информации путем применения существующих средств защиты вследствие их несовершенства или несоответствия современному уровню развития средств несанкционированного доступа к информации;
* Отказы — совокупность факторов, приводящих к потере системой защиты или одним из средств защиты способности выполнять свои функции;
* Сбои — совокупность факторов, приводящих к кратковременному нарушению работы средств зашиты или выходу характеристик их работы за допустимые интервалы значений;
* Ошибки операторов СЗИ — совокупность факторов, приводящих к нарушению технологии автоматизированной обработки информации в СЗИ вследствие некорректных действий операторов;
* Стихийные бедствия — совокупность факторов, приводящих к утечке информации вследствие физического разрушения элементов СИЗ при воздействии на них сил природы без участия человека.
* Злоумышленные действия — совокупность факторов, приводящих к изменению режимов функционирования СЗИ, уничтожению, искажению или раскрытию информации в результате непосредственного целенаправленного воздействия нарушителя на компоненты СЗИ.

Нейтрализация угроз осуществляется следующими методами:

* блокировка ответа при неправильном числе запросов
* искажение ответа путем округления и другой преднамеренной коррекции данных
* разделение баз данных
* случайный выбор записи для обработки
* контекстно-ориентированная защита
* контроль поступающих запросов.

**Задание № 4:**



где к – число угроз; n – число нарушителей; Рi – вероятность появления субъекта i-го типа; p(j/i) – условная вероятность того, что субъект i-го типа выберет для реализации угрозу j-го типа; qн1– вероятность несрабатывания средств обнаружения; qн2 – вероятность несрабатывания средств отражения; а – постоянная величина, характеризующая "скорость" реализации угрозы, tот – время, которым располагает субъект угрозы, если tот = 0 – угроза не реализуется.

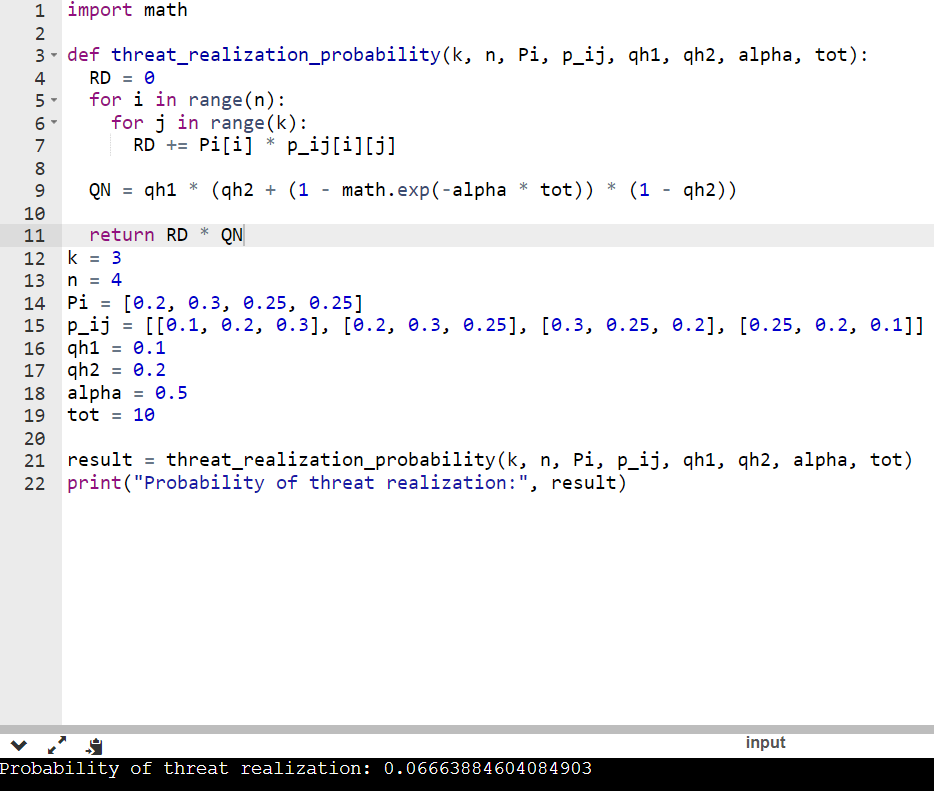


Рисунок 1. Программа по подсчету общей вероятности нарушения безопасности объекта

**Задание № 5**:

Обеспечение конфиденциальности и целостности данных;

1. Определение и оценка наиболее вероятных угроз и рисков для информационной системы и ее данных;
2. Защита от несанкционированного доступа к системе;
3. Использование безопасных протоколов передачи данных;
4. Шифрование информации;
5. Организация контроля доступа к ресурсам системы;
6. Обеспечение резервного копирования данных;
7. Установка антивирусного ПО и регулярное обновление баз;
8. Обучение и информирование пользователей о мерах безопасности;
9. Регулярная проверка и мониторинг системы на наличие уязвимостей и их устранение;
10. Физическая безопасность серверов;
11. Установление требований к аутентификации, авторизации и управлению доступом;
12. Создание и документирование правил и процедур, обеспечивающих безопасность информационной системы.

Задание № 6 Выберите методы и средства защиты информации для исследуемой информационной системы.

Информационная система турагентства может использовать следующие методы и средства защиты информации:

1 Шифрование данных: использование алгоритмов шифрования для защиты данных при передаче и хранении.

2 Аутентификация и авторизация пользователей: подлинности пользователя и предоставление ему доступа только к тем данным, к которым у него есть разрешение.

3 Разграничение доступа: разделение информации на разные уровни доступа, в зависимости от роли пользователя в системе.

4 Резервное копирование данных: создание копий данных для восстановления в случае их потери.

5 Антивирусное программное обеспечение: защита от вредоносных программ и вирусов.

6 Физическая безопасность: обеспечение безопасности помещения, где находится оборудование информационной системы.

**Выводы:**

В ходе работы я получил навыки разработки требований безопасности информационной системы.