Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И ЭЛЕКТРОНИКИ (ТУСУР)

Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)

МОДЕЛИРОВАНИЕ УГРОЗ, НАПРАВЛЕННЫХ НА ИНФОРМАЦИОННЫЙ ПРОЦЕСС

Отчет о практической работе №2

по дисциплине «Основы информационной безопасности»

Студент гр. 712-1

_____А.Г. Будаев

_____

Руководитель

Преподаватель кафедры КИБЭВС

_____ _____ В.С. Агеева

_____

Томск 2023

Введение

Целью практической работы является получение навыков комплексного моделирования угроз, учитывающего угрозы, направленные на информационную систему и обрабатываемую ей информацию.

Задачи:

1. На основе IDEF0 модели процесса, обрабатывающего защищаемую информацию, выделить перечень защищаемых и классифицировать их на три типа – информационные элементы, исполнители, управление.
2. Привести по одному примеру угроз конфиденциальности, целостности и доступности для каждого информационного элемента.
3. Привести по одному примеру угроз конфиденциальности, целостности для каждого механизма реализации процесса.
4. Привести по одному примеру угроз конфиденциальности, целостности для каждого элемента управления процессом.

Ход работы

1 Выделение и классификация защищаемых элементов

На основе IDEF0 модели информационного процесса (рисунок 1), обрабатывающего защищаемую информацию, выделяем перечень защищаемых элементов и разделяем их на три типа (информационные элементы, исполнители и управление) следующим образом:

1. Информационные элементы:
    a. БД военкомата;
    b. Повестка;
    c. Приписное свидетельство;
    d. Документ удостоверяющий личность (паспорт);
    e. Справка из ВУЗа;
2. Исполнители:
    a. Призывник;
    b. Сотрудник военкомата.
3. Управление:
    a. ФЗ «О воинской обязанности и военной службе»;
    b. Правила заполнения документов;
    c. Крайний срок обновления БД о получивших отсрочку студентах.

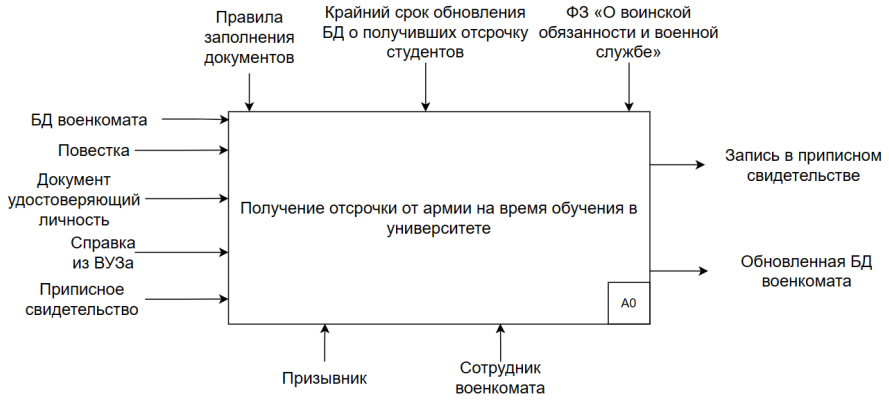

Рисунок 1 – Модель информационно процесса

Далее для каждого защищаемого элемента, находящегося на горизонтальных стрелках, в таблице 1 представлены потенциальные угрозы, нарушающие принципы триады CIA, а также организационные и технические меры защиты.

Таблица 1 – Угрозы на горизонтальные стрелки

Объект/ элемент	Угрозы	Нарушения в ходе реализации угроз	Организационные меры защиты	Технические меры защиты
Горизонтальные стрелки				
БД Воен-комата	Несанкционированное копирование БД на мобильный носитель	Конфиден-циальность	Внедрение требований по обеспечению ИБ при обращении с мобильными носителями	Контроль за подключаемыми мобильными носителями на рабочей станции
	Несанкционированное изменение/удаление информации	Целостность	Информирование сотрудников об ответственности за нарушение целостности информации	Система внутреннего контроля пользователей
	Потеря доступа к базе данных вследствие заражения системы вредоносной программой	Доступность	Провести комплекс мероприятий по антивирусной защите и аудиту	Обновление антивирусного ПО
При-писное	Несанкционированное	Конфиден-циальность	Не оставлять документ без	Внедрение комплексного

	сканирование документа		присмотра	Anti-Leakage Software
	Непреднамеренное намокание документа	Целостность	Не работать с документом рядом с жидкостями	Ламинирование документа
	Потеря приписного свидетельства	Доступность	Повышение контроля за своими документами	GPS-метка, для отслеживания местоположения документа
Повестка	Непреднамеренное раскрытие личной информации из повестки на улице	Конфиден-циальность	Разработка и принятие мер направленных на борьбу со случайными утечками	-
	Неверные данные в документе	Целостность	Проверка документа на корректность формы после получения	-
	Утрата документа в ходе доставки	Доступность	Ответственный подход к выбору курьера	
Доку-метн УЛ	Утечка БД клиентов онлайн-платформы для заказа еды	Конфиден-циальность	Ужесточение наказания за утечку персональных данных	Использование SIEM системы
	Утрата одной или нескольких страниц документа	Целостность	Аккуратное использование документов	Обложка на документ УЛ
	Кража документа УЛ	Доступность	Ответственно подходить к выбору места для прогулки ночью	Внутренний карман одежды
Справка из ВУЗа	Несанкционированно е распространение данных справки из ВУЗа	Конфиден-циальность		
	Не пропечатанный текст в документе	Целостность	Регулярная проверка краски в принтере	Закупка нового оборудования для печати
	Потеря документа в следствии природного катаклизма	Доступность	Просмотр отчетов метеоцентров об надвигающихся природных угрозах	Строительство бункера на заднем дворе с системой защиты от природных катаклизмов

Далее для каждого защищаемого элемента, находящегося на вертикальных стрелках, в таблице 2 и 3 представлены потенциальные угрозы, нарушающие принципы конфиденциальности и целостности, а также организационные и технические меры защиты.

Таблица 2 – Угрозы на нижние стрелки

Объект/ элемент	Угрозы	Нарушения в ходе реализации угроз	Организационные меры защиты	Технические меры защиты
Нижние стрелки				
Призыв-ник	Разглашение личной информации	Конфиден-циальность	Хранение личной информации в тайне	Двухфакторная аутентификация на личных аккаунтах
	Появление травмы	Целостность	Инструктаж техники безопасности	Обеспечение безопасности посетителей учреждения
Сотруд-ник	Компрометация личных данных	Конфиден-циальность	Информирование сотрудников об ИБ угрозах	Использование менеджеров паролей
	Потеря конечностей	Целостность	Инструктаж об оказании первой помощи	Создание комфортных условий труда

Таблица 3 – Угрозы на верхние стрелки

Объект/ элемент	Угрозы	Нарушения в ходе реализации угроз	Организационные меры защиты	Технические меры защиты
Верхние стрелки				
Правила запол-нения доку-ментов	Общедоступная информация	Конфиден-циальность	Контроль за принятием новых правил	-
	Несанкционированная модификация правил заполнения документов	Целостность	Курсы повышения квалификации работников	Архивация корпоративного документооборота
Крайний срок обнов-ления БД	Несанкционированное распространение информации	Конфиден-циальность	Договор о неразглашении информации	Контроль почтового и веб-трафика
	Несанкционированные изменение крайнего срока обновление БД	Целостность	Архивация документов	Разграничение прав доступа к данным

ФЗ «О воинской обязанности и военной службе»	Общедоступная информация	Конфиденциальность	Соблюдение регламента принятия ФЗ	-
	Несанкционированное переформулирование пунктов ФЗ	Целостность	Проверка структуры документа	Использование средств защиты информации

Заключение

В ходе практической работы были освоены навыки комплексного моделирования угроз, что включает в себя анализ системы на наличие потенциальных угроз, а также подбор необходимых организационных и технических мер защиты.