МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФГБОУ ВО «АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт цифровых технологий, электроники и физики (ИЦТЭФ)
Кафедра вычислительной техники и электроники (ВТиЭ)

Лабораторная работа №3

Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности

Выполнил студент 595 гр.
_____ В.В. Борисов
Проверил:
_____ Ладыгин П.С.
Оценка _____
«____» _____2023 г.

Барнаул 2023

Цель работы:

Продолжение знакомства с документом «Методика оценки угроз безопасности информации», а также подготовка к созданию модели нарушителя персональной информационной системы.

1. Определить виды нарушителей, актуальные для персональной ИС.

1.1. Используя таблицу «Возможные цели реализации угроз безопасности информации нарушителями», полученную в лабораторной работе №2, оценить цели реализации данных угроз. Для этого необходимо составить таблицу по примеру из Приложения 7 «Методики оценки угроз безопасности» (Учесть, что в нашем частном случае актуально только «нанесение ущерба физическому лицу»)

Виды нарушителей	**Нанесение ущерба физ. Лицу(возможные цели реализации угроз безопасности информации)**	**Соответствие целей видам риска(ущерба) и возможным негативным последствиям**
Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)	Нарушение личной неприкосновенности , финансовый ущерб физ.лицу, нарушение конфиденциальности персональных данных
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ	Разглашение персональных данных граждан, нарушение конфиденциальности персональных данных
Авторизованные пользователи систем и сетей	Непреднамеренные, неосторожные или неквалифицированные действия. Любопытство или желание самореализации	(финансовый, иной материальный ущерб физическим лицам)

1.2. Используя таблицу «Уровни возможностей нарушителей по реализации угроз безопасности информации» (с.56-59), составить таблицу по примеру на с. 60.

Виды риска(ущерба) и возможные негативные последствия	**Виды актуального нарушителя**	**Категория нарушителя**	**Уровень возможностей нарушителя**
Нарушение личной неприкосновенности , финансовый ущерб физ.лицу, нарушение конфиденциальности персональных данных. Разглашение персональных данных граждан, нарушение конфиденциальности персональных данных. Унижение достоинства личности, нарушение личной, семейной тайны, утрата чести и доброго имени, нарушение тайны переписки, телефонных переговоров, иных сообщений, недополучение ожидаемой прибыли, необходимость дополнительных затрат на восстановление деятельности	Отдельные физические лица(хакеры)	Внешний	H2
	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	H1

Непреднамеренные, неосторожные или неквалифицированные действия. Любопытство или желание самореализации	Авторизованные пользователи систем и сетей	Внутренний	H1

2. Определить актуальные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности.

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Отдельные физические лица(хакеры)	Внешний	Удаленное автоматизированное рабочее место (АРМ) пользователя: несанкционированный доступ к операционной системе АРМ пользователя; нарушение конфиденциальности информации, содержащейся на АРМ пользователя	Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Съемные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя
				Сетевые интерфейсы коммутатора сети, где расположен веб-сервер	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя
2	Лица, обеспечивающие поставку	Внешний	Удаленное автоматизированное рабочее	Пользовательский веб-интерфейс	Использование уязвимостей конфигурации

	программных, программно-аппаратных средств, обеспечивающих систем		место (АРМ) пользователя: несанкционированный доступ к операционной системе АРМ пользователя; нарушение конфиденциальности информации, содержащейся на АРМ пользователя	доступа к базе данных информационной системы	системы управления базами данных
3	Авторизованные пользователи систем и сетей	Внутренний	Рабочее место (АРМ) пользователя: несанкционированный доступ к операционной системе АРМ пользователя; нарушение конфиденциальности информации, содержащейся на АРМ пользователя	Локальная вычислительная сеть	Изучение литературы, следование простым инструкциям
				Съемные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя
				Внешние интерфейсы управление системой(мышь и клавиатура)	Ожидание, пока место не станет свободным и физическое взаимодействие со стулом

Ответы на контрольные вопросы:

1. С какими видами нарушителей вы встречались в своей практике пользования ИС?

Отдельные физические лица(хакеры), лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора(администрация)

2. Опишите три любых сценария утечки данных из вашей ИС (количество слов в каждом сценарии не менее 50)

1. Читаю почту, тут вижу сообщение с темой: «МВидео раздает подарки!» в папке спам. Разумеется, я кликаю на сообщение, по инструкции в письме ввожу персональные данные своей странички или еще чего-нибудь. Тут то я и попадаюсь на уловку мошенников, данные моего личного кабинета от МВидео в ненадежных руках и с накопленными баллами за покупки я могу попрощаться.

2. Я скачиваю приложение «Сбербанк взлом 100%» предвкушая легкий кэш. Приложение просит у меня ввести фотографию моего паспорта чтобы попасть в личный кабинет. Я добросовестно кидаю фотографию из галереи, захожу в приложение и оказывается, что оно работает плохо. Мои данные почему-то не дошли до сервера или введены неправильно. Странно, но сбербанк взломать не удалось. Через 2 часа приходит сообщение: «На вас оформлен кредит в размере 100 тугриков». За моим окном притормаживает черный воронок с бритоголовыми уголовниками.

3. Я отхожу от своего рабочего места на кухню в поисках еды. В это время мой сосед беззастенчиво подходит к моему компьютеру, делает снимок рабочего стола, затем через флешку выкачивает гигабайты моих смешных картинок, которые я так долго копил. После удаляет все ярлыки с рабочего стола и ставит как фон рабочего стола недавно сделанный снимок рабочего стола. В это время с возвращаюсь с кухни, не найдя еды и пребывая в тяжелом состоянии, сажусь за рабочее место, пытаюсь открыть «Этот компьютер», но он почему-то не открывается. Маятник душевного равновесия грозит качнуться в «правильную» сторону. Путем прямого перехода в свою папку с картинками я замечаю ее пустой, стул подо мной плавится по неустановленным причинам, за спиной слышатся издевательские реплики соседа, мой желудок урчит, а день еще только начался. Занавес.