МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

Институт кибербезопасности и цифровых технологий
Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Отчёт по практической работе № 1.10

По дисциплине

«Управление информационной безопасностью»

Тема: «Расчёт рисков информационной безопасности»

Студент Кузькин Павел Александрович

Группа ББМО-01-22

Работу проверил

Пимонов Р.В.

Москва, 2023

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИС – Автоматизированная информационная система

АРМ – Автоматизированное рабочее место

АПМДЗ – Аппаратно-программный модуль доверенной загрузки

БД – База данных

ИСПДн – Информационная система персональных данных

ЛВС – Локальная вычислительная сеть

НИЦ – Национальный исследовательский центр

НСД – Несанкционированный доступ

ПДн – Персональные данные

ПИЯФ – Петербургский институт ядерной физики им. Б.П. Константинова

ФГБУ – Федеральное государственное бюджетное учреждение

РАСЧЁТ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной практической работе производится расчёт рисков информационной безопасности для автоматизированной информационной системы ФГБУ «ПИЯФ» НИЦ «Курчатовский институт». Входные данные по ресурсам, угрозам и уязвимостям ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» представлены в таблице 1.

Таблица 1 – Входные данные по ресурсам, угрозам и уязвимостям ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»

Ресурс	Угрозы	Уязвимости
Ресурс 1 ИСПДн АИС ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»	Угроза 1 НСД к ресурсам ИСПДн	Уязвимость 1 Отсутствие АПМДЗ
		Уязвимость 2 Отсутствие автоматической блокировки АРМ при отсутствии сотрудника на рабочем месте
	Угроза 2 Утечка конфиденциальной информации или отдельных файлов (нарушение конфиденциальности)	Уязвимость 1 Уволенные сотрудники
		Уязвимость 2 Недостаточные санкции, нечёткие формулировки в регламенте о разглашении информации
Ресурс 2 ЛВС, в рамках которой работники обеспечивают обмен информацией	Угроза 1 Угроза подмены ip-адреса с последующей возможностью проведения атаки mitm	Уязвимость 1 Используется динамическая маршрутизация
		Уязвимость 2 Недостаточные настройки списков доступа (ACL) на маршрутизаторах

	Угроза 2 Эскалация привилегий злоумышленником в ЛВС	Уязвимость 1 Недостаточная настройка доменных систем ЛВС
Ресурс 3 Сервер, на котором хранятся БД ИСПДн, АИС ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»	Угроза 1 Отказ в обслуживании сервера (нарушение доступности)	Уязвимость 1 Отсутствие механизмов защиты от DoS/DDoS
		Уязвимость 2 Не реализовано резервирование сервера
	Угроза 2 НСД к серверу, на котором хранятся БД ИСПДн	Уязвимость 1 Отсутствие двухфакторной аутентификация при слабых/скомпрометированных паролях

Отобразим вероятности реализации угрозы через уязвимость в течение года и критичности реализации угрозы через данную уязвимость для каждого ресурса ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» в таблице 2.

Таблица 2 – Входные данные для расчёта рисков информационной безопасности для автоматизированной информационной системы ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»

Ресурс 1. ИСПДн АСИ ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»		
Угроза/уязвимость	Вероятность реализации угрозы через уязвимость в течении года %, P(V)	Критичность реализации угрозы через данную уязвимость %, ER
Угроза 1 /Уязвимость 1	70	80
Угроза 1 /Уязвимость 2	20	30
Угроза 2 /Уязвимость 1	10	40
Угроза 2 /Уязвимость 2	30	50

Ресурс 2. ЛВС, в рамках которой работники обеспечивают обмен информацией		
Угроза/уязвимость	Вероятность реализации угрозы через уязвимость в течении года %, P(V)	Критичность реализации угрозы через данную уязвимость %, ER
Угроза 1 /Уязвимость 1	30	60
Угроза 1 /Уязвимость 2	50	70
Угроза 2 /Уязвимость 1	50	50
Ресурс 3. Сервер, на котором хранятся БД ИСПДн, АСИ ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»		
Угроза/уязвимость	Вероятность реализации угрозы через уязвимость в течении года %, P(V)	Критичность реализации угрозы через данную уязвимость %, ER
Угроза 1 /Уязвимость 1	60	80
Угроза 1 /Уязвимость 2	70	80
Угроза 2 /Уязвимость 1	40	50

Отобразим результаты расчёта уровня угрозы по каждой уязвимости, уровня угрозы по всем уязвимостям, через которые она может быть реализована, общего уровня угроз по ресурсу и риска по ресурсу для каждого ресурса ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» в таблице 3.

Таблица 3 – Итоги расчёта показателей Th, CTh, CThR и R для каждого ресурса ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»

Ресурс 1. ИСПДн АСИ ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»				
Угроза/уязвимость	Уровень угрозы по каждой уязвимости %, Th	Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh	Общий уровень угроз по ресурсу %, CThR	Риск по ресурсу у.е., R
Угроза 1 /Уязвимость 1	0,56	0,5864	0,6625024	66,25024
Угроза 1 /Уязвимость 2	0,06			
Угроза 2 /Уязвимость 1	0,04	0,184		

Угроза 2 /Уязвимость 2	0,15			
Ресурс 2. ЛВС, в рамках которой работники обеспечивают обмен информацией				
Угроза/уязвимость	Уровень угрозы по каждой уязвимости %, Th	Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh	Общий уровень угроз по ресурсу %, CThR	Риск по ресурсу у.е., R
Угроза 1 /Уязвимость 1	0,18	0,467	0,60025	60,025
Угроза 1 /Уязвимость 2	0,35			
Угроза 2 /Уязвимость 1	0,25	0,25		
Ресурс 3. Сервер, на котором хранятся БД ИСПДн, АСИ ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»				
Угроза/уязвимость	Уровень угрозы по каждой уязвимости %, Th	Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh	Общий уровень угроз по ресурсу %, CThR	Риск по ресурсу у.е., R
Угроза 1 /Уязвимость 1	0,48	0,7712	0,81696	81,696
Угроза 1 /Уязвимость 2	0,56			
Угроза 2 /Уязвимость 1	0,2	0,2		

Таким образом, в результате расчётов риск по ресурсам (CR) равен 207,97124 условных единиц. Исходя из расчетов, видно, что риск реализации по трём угрозам выше среднего. Также высока реализация данных угроз для выбранных ресурсов. Из полученных данных можно понять, что необходимо пересмотреть политику безопасности в организации, а также улучшить меры защиты объектов, связанных с информацией.

РЕКОМЕНДАЦИИ

1. Выполнить установку АПМДЗ на всех точках взаимодействия человека с вычислительной техникой ФГБУ «ПИЯФ» НИЦ «Курчатовский институт».

2. Настроить статическую маршрутизацию, даже если это займёт значительное количество времени.

3. Реализовать механизм блокировки рабочего стола АРМ при отсутствии человека на рабочем месте.

4. Выполнить кластеризацию сервера (зарезервировать), на котором хранятся БД ИСПДн, АИС ФГБУ «ПИЯФ» НИЦ «Курчатовский институт».

5. Помимо АПМДЗ, необходимо реализовать двухфакторную аутентификацию, например, через номер телефона.

6. Реализовать механизмы защиты от Dos/DDoS атак, например, установить утилиту Fail2ban.

7. Внести правки в регламент о разглашении информации, чтобы изложенная там информация была понятна читателю. Санкции в этом документе должны однозначно отбивать желание поделиться с кем-либо конфиденциальной информацией.

8. Внедрить сканер уязвимостей, который бы указывал администраторам информационной безопасности на “дыры” в списках доступа на маршрутизаторах и на уязвимости доменной системы ЛВС ФГБУ «ПИЯФ» НИЦ «Курчатовский институт».