

«Обеспечение информационной безопасности информационной системы библиотеки»

по дисциплине: «Управление информационной безопасностью»

Этап 1. Описание объекта (бизнес-процессы организации, процессы объекта, идентификация активов)

Группа М17-505

Команда №7

Студент: Майоров Анатолий

Преподаватель: Толстой Александр Иванович

Цель: описать ИС библиотеки с точки зрения информационной безопасности, определить бизнес-процессы библиотеки, процессы ИС библиотеки, идентифицировать активы.

Задачи:

- Определить функции организации
- Составить схему функционирования библиотеки
- Определить особенности инфраструктуры ИС библиотеки
- Связать активы с процессами и элементами инфраструктуры

Функции библиотеки

Библиотека осуществляет деятельность по хранению, выдаче и приему книг у клиентов.

Дополнительно, библиотека осуществляет свою деятельность через интернет-портал, на котором клиенты могут осуществлять поиск и резервирование книг.

Интернет-портал повышает удобство пользования библиотекой, позволяя клиентам удаленно выбрать интересующую книгу и выполнить её резервирование.

Бизнес-процессы библиотеки

Регистрация клиентов

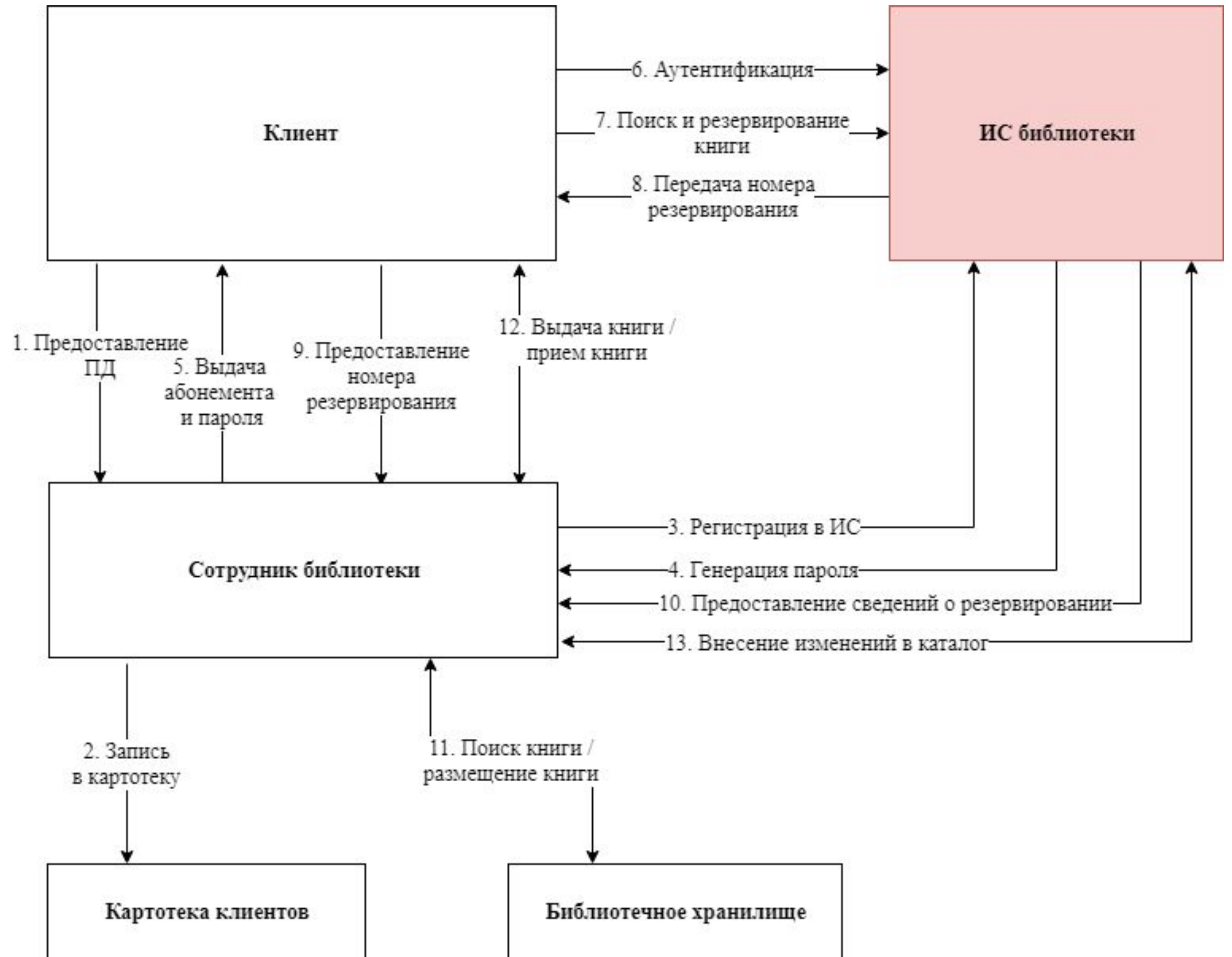
Хранение книг

Выдача книг

Прием книг

Резервирование книг
для клиентов

Схема функционирования библиотеки



Основные процессы ИС библиотеки

Регистрация
пользователей

Аутентификация
пользователей

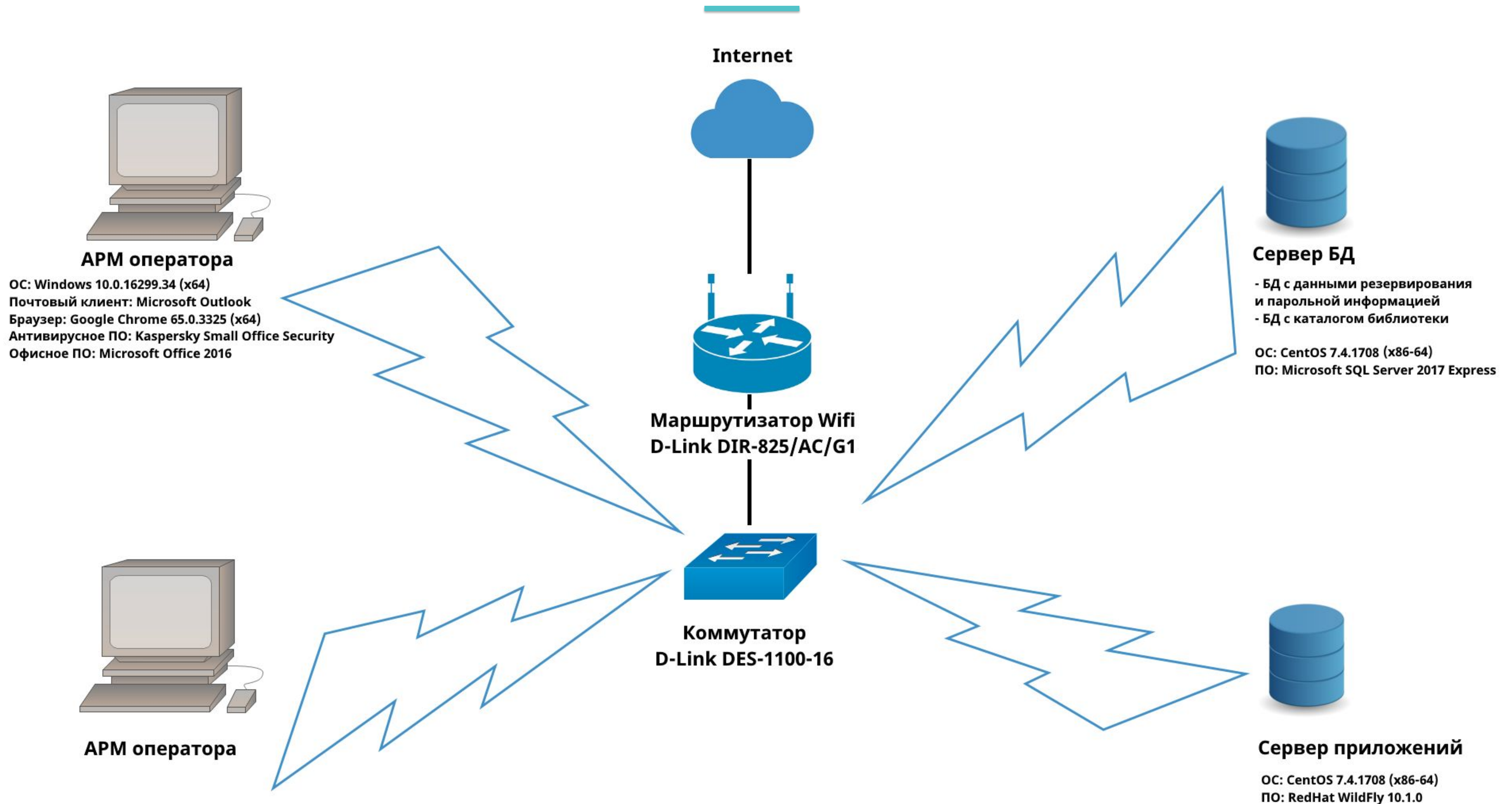
Поиск книг в
электронном каталоге

Резервирование
книг

Предоставление
информации
о резервировании

Внесение изменений
в электронный каталог

Инфраструктура ИС библиотеки



АКТИВЫ

Информационные активы

- Парольная информация клиентов
- Электронный каталог библиотеки
- Информация о резервах книг

Среда, обрабатывающая информационные активы

- БД с данными резервирования, парольной информацией.
- БД с каталогом библиотеки.
- Каналы связи.
- Серверное, сетевое и служебное оборудование.
- Программное обеспечение (системное, прикладное).

Связь бизнес-процессов библиотеки с активами (1)

Процесс, реализуемый в организации	Элемент инфраструктуры	Информационный актив (ИА)		Актив, относящийся к объекту среды обработки ИА	
		Тип актива	Уязвимости	Тип актива	Уязвимости
Регистрация/аутентификация пользователей	Сервер с БД	Парольная информация пользователей	К, Ц, Д	БД с данными резервирования, парольной информацией	1. Уязвимость к SQL-Injection 2. Неверное разграничение прав доступа
Поиск книг в электронном каталоге /резервирование книг	Сервер с БД	Электронный каталог библиотеки	Ц, Д	БД с каталогом библиотеки	1. Уязвимость к SQL-Injection 2. Уязвимость к XSS-атаке
		Информация о резервах	К, Ц, Д	БД с данными резервирования, парольной информацией	1. Уязвимость к SQL-Injection 2. Неверное разграничение прав доступа
Предоставление информации о резервировании	Сервер с БД	Информация о резервах	К, Ц, Д	БД с данными резервирования, парольной информацией	1. Уязвимость к SQL-Injection 2. Неверное разграничение прав доступа
Внесение изменений в электронный каталог	Сервер с БД	Электронный каталог библиотеки	Ц, Д	БД с каталогом библиотеки	1. Уязвимость к SQL-Injection 2. Уязвимость к XSS-атаке

Связь бизнес-процессов библиотеки с активами (2)

Процесс, организуемый в организации	Элемент инфраструктуры	Активы, не отнесенные к ИА		
		Тип актива	Уязвимости	Свойства, приоритеты
Регистрация/аутентификация пользователя	Сервер приложений	Серверы приложений /БД	1. Отсутствие и/или неправильная настройка программно-аппаратных СЗИ	Ц
			1. Незащищенность от преднамеренные действия пользователей, имеющих доступ	Ц, Д
			2. Возможность непреднамеренных действий пользователей	
		1. Уязвимость к DoS/DDoS атаке	Д	
	Линии связи	Каналы связи	1. Уязвимость к несанкционированному анализу сетевого трафика	К
	АРМ операторов	Программное обеспечение (системное, прикладное)	1. Уязвимость к преднамеренным действиям пользователей 2. Уязвимость к непреднамеренным действиям пользователей	Ц, Д

Связь бизнес-процессов библиотеки с активами (3)

Процесс, организуемый в организации	Элемент инфраструктуры	Активы, не отнесенные к ИА		
		Тип актива	Уязвимости	Свойства, приоритеты
Поиск книг в электронном каталоге /резервирование книг	Сервер приложений	Серверы приложений /БД	1. Отсутствие и/или неправильная настройка программно-аппаратных СЗИ	Ц
			1. Незащищенность от преднамеренные действия пользователей, имеющих доступ	Ц, Д
			2. Возможность непреднамеренных действий пользователей	
		1. Уязвимость к DoS/DDoS атаке	Д	
	Линии связи	Каналы связи	1. Уязвимость к несанкционированному анализу сетевого трафика	К

Связь бизнес-процессов библиотеки с активами (4)

Процесс, организуемый в организации	Элемент инфраструктуры	Активы, не отнесенные к ИА		
		Тип актива	Уязвимости	Свойства, приоритеты
Предоставление информации о резервировании	Сервер приложений	Серверы приложений /БД	1. Отсутствие и/или неправильная настройка программно-аппаратных СЗИ	Ц
			1. Незащищенность от преднамеренные действия пользователей, имеющих доступ	Ц, Д
			2. Возможность непреднамеренных действий пользователей	
	1. Уязвимость к DoS/DDoS атаке	Д		
	АРМ операторов	Программное обеспечение (системное, прикладное)	1. Уязвимость к преднамеренным действиям пользователей 2. Уязвимость к непреднамеренным действиям	Ц, Д

Связь бизнес-процессов библиотеки с активами (5)

Процесс, организуемый в организации	Элемент инфраструктуры	Активы, не отнесенные к ИА		
		Тип актива	Уязвимости	Свойства, приоритеты
Внесение изменений в электронный каталог	Сервер приложений	Серверы приложений /БД	1. Отсутствие и/или неправильная настройка программно-аппаратных СЗИ	Ц
			1. Незащищенность от преднамеренные действия пользователей, имеющих доступ	Ц, Д
			2. Возможность непреднамеренных действий пользователей	
	1. Уязвимость к DoS/DDoS атаке	Д		
АРМ операторов	Программное обеспечение (системное, прикладное)	1. Уязвимость к преднамеренным действиям пользователей 2. Уязвимость к непреднамеренным действиям пользователей 3. Устаревшее ПО 4. Возможность внедрения вредоносного ПО	Ц, Д	

Благодарю за внимание!