УДК 004.056:027.7 **Технические науки**

Федякова Наталия Николаевна, *к.э.н, доцент кафедры статистики, эконометрики и информационных технологий в управлении,*
Ивойлов Эльдар Михайлович, *студент 2 курса*
Табачников Роман Андреевич, *студент 2 курса*
ФГБОУ ВО «МГУ им. Н.П. Огарева», Саранск

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ

Аннотация. В данной статье рассмотрено обеспечение информационной безопасности сервиса «Электронная библиотека». Выявлены наиболее значимые угрозы безопасности информации для Электронной библиотеки. Обозначены основные задачи информационной безопасности. Рассмотрены требования и правила политики информационной безопасности, источники угроз для защищаемого объекта, а также основные аспекты действий по реагированию в конкретных ситуациях по предотвращению DDoS атак.

Ключевые слова: информационная безопасность, электронная библиотека, DDoS атака.

Annotation This article describes the information security of the service "Electronic library". Identified the most significant threats to information security for the Electronic library. The main tasks of information security. Reviewed requirements and policies for information security, sources of threats to the protected object, as well as the main aspects of the response in specific situations to prevent DDoS attacks.

Keywords: information security, e-library, DDoS attack.

Электронная библиотека предоставляет пользователям дистанционный доступ к информационной и платежной подсистемам библиотеки после процедуры регистрации пользовательской учетной записи.

Ознакомимся с перечнем защищаемых активов при использовании данной системы. В электронной библиотеке предусмотрены такие активы, как базы данных (пользователей, финансовой отчетности, событий и инцидентов, произведений авторов), веб-сайты, оборудование (серверное, сетевое, служебное), и так же программное обеспечение (ПО), используемое администратором.

Современная электронная библиотека - это целый комплекс тесно связанных друг с другом, сложных информационных систем, каждая из которых нуждается в обеспечении информационной безопасности.

Для обеспечения безопасности Электронной библиотеки, при корректном функционировании информационной системы, администраторами сервиса регулярно проводится анализ угроз. Все результаты данных тестов документируются. Создаются модели угроз системы, а также нарушителей безопасности.

Модели угроз описывают источники угроз для Электронной библиотеки, уязвимостей, используемых угрозами, способов нападений и типы возможных потерь и масштабов возможного ущерба.

Для улучшения и развития безопасности сервиса модели угроз и модели нарушителей являются основными средствами.

В таблице 1 приведены возможные источники угроз для защищаемого объекта [1].

Таблица 1 - Источники угроз для защищаемого объекта**.**

Угроза	**Актив подвергающийся угрозе**	**Возможный способ реализации угрозы**	**Нарушаемое свойство актива**	**Уровень модели ОСИ**	**Вероятность реализации угрозы**	**Нарушитель**
Сетевая	БД	DoS/DDoS	Доступность	Прикладной, транспортный, сетевой	Высокая	Внешний
		Использование вредоносного ПО	Целостность, доступность, конфиденциальность	Прикладной	Высокая	Внешний
		SQL-инъекция	Целостность, доступность, конфиденциальность	Прикладной	Средняя	Внешний
	Веб-сайт	DoS/DDoS	Доступность	Прикладной, транспортный, сетевой	Высокая	Внешний
		SQL-инъекция	Целостность, доступность, конфиденциальность	Прикладной	Средняя	Внешний
		XSS-атака	Целостность, доступность, конфиденциальность	Прикладной	Средняя	Внешний
	ПО	Использование вредоносного ПО	Целостность, доступность	Прикладной	Высокая	Внешний
Хищение/ порча оборудования	Оборудование	Физические действия злоумышленника	Целостность, доступность, конфиденциальность	-	Низкая	Внутренний
АРМ администратора	БД	Хищение/удаление/изменение информации	Целостность, доступность, конфиденциальность	-	Низкая	Внутренний
	Оборудование	Аппаратная закладка	Целостность, доступность, конфиденциальность	-	Низкая	Внутренний
	ПО	Использование вредоносного ПО	Целостность, доступность, конфиденциальность	-	Низкая	Внутренний

Политика информационной безопасности определяет общие направления, цели и задачи обеспечения информационной безопасности системы Электронной библиотеки, а также основные принципы и общие требования к организации процессов обеспечения информационной безопасности при использовании системы электронной библиотеки.

Основным защищаемым ресурсом в сети электронной библиотеки является информация в цифровом виде, хранящаяся в предусмотренных базах данных и передаваемая по каналам связи между пользователями сервиса и сервером. Отсюда главной целью является обеспечение и постоянное поддержание следующих свойств информации:

– доступность информации для легитимных пользователей Электронной библиотеки;

– целостность и аутентичность информации, хранимой и обрабатываемой в информационной системе и передаваемой по каналам связи;

– конфиденциальность информации [3].

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается соответствующими множеству угроз методами и средствами.

Сервис предоставляет пользователям дистанционный доступ к подсистемам библиотеки после процедуры регистрации пользовательской учетной записи.

Регистрационные учетные записи:

- обычные – бесплатные подписки, предоставляющие доступ к ограниченному объему информации, расположенной на веб-сайте Электронной библиотеки;
- VIP – платные подписки, предоставляющие доступ к полному объему информации, расположенной на веб-сайте Электронной библиотеки;
- авторские – платные подписки, предоставляющие авторам возможность размещать свои произведения на сайте.

Каждому пользователю присваивается уникальная пользовательская регистрационная учетная запись.

Такой вид доступа подвержен различным угрозам, которым необходимо противостоять.

Основные функции электронной библиотеки:

- обеспечение круглосуточного онлайн-доступа к чтению электронных книг, хранящихся на едином сервере;
- возможность приобретения платного абонемента с дополнительными привилегиями (незамедлительный доступ ко всем новинкам, опубликованным на ресурсе и др.);
- добавление книг на единый сервер;
- автоматизированный поиск и обработка ресурсов Электронной библиотеки;
- возможность обсуждения книг пользователями;
- поддержка конфиденциальности, аутентичности и неотказуемости от авторства.

Основные группы риска:

- Веб-сайт;
- сервер и информационные ресурсы, хранящиеся на нем;
- система платежей.

Типовой состав участников Электронной библиотеки:

- серверное, сетевое и служебное оборудование;
- каналы связи;
- программное обеспечение (системное, прикладное);
- информация (электронные книги, персональные данные, платежи);
- люди (администратор ресурса, пользователи);
- используемые процессы, процедуры (разработка, внедрение, сопровождение);
- помещение, используемое для работы оборудования.

Наиболее значимыми угрозами безопасности информации для Электронной библиотеки являются сетевые угрозы, хищение и порча оборудования, несанкционированный доступ к рабочему месту администратора, серверу и сетевому оборудованию.

Основными задачами ИБ являются:

1. Разграничение доступа пользователей к информационным ресурсам электронной библиотеки.
2. Организация мероприятий по предотвращению сетевых атак и внедрения вредоносного ПО.
3. Обеспечение целостности структуры Веб-сайта.

4. Правила пользования устройствами и техническими средствами сети Электронной библиотеки.

5. Для повышения эффективности обеспечения ИБ организовать систему управления безопасности [4].

Рассмотрим требования и правила политики ИБ. В рамках организации обеспечения ИБ Электронной библиотеки необходимым является наличие системы управления информационной безопасности (СУИБ) – системы, предназначенной для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности Электронной библиотеки.

Для успешного функционирования СУИБ Электронной библиотеки должны быть реализованы следующие процессы:

- система мониторинга событий;
- система управления инцидентами ИБ.

Система управления информационной безопасностью базируется на системе мониторинга событий информационной безопасности, которое обеспечивает выявление всех событий, касающихся системы электронной библиотеки, таких как авторизация, регистрация пользователей, запросы пользователей на веб-сервер и ответы сервера, загрузка на сервер персональных данных, произведений авторов и других идентификационных данных, и системе управления инцидентами информационной безопасности, которая включает в себя выявление инцидентов информационной безопасности и необходимые процедуры по их обработке, хранению и анализу.

Доступ пользователей к ресурсам Электронной библиотеки должен соблюдаться правилами, в рамках которых формулируются процедуры создания, изменения, удаления учетных записей пользователей, правила хранения и содержания идентификационных и персональных данных пользователей в БД.

Для минимизации уровня сетевых угроз необходимо руководствоваться сведениями, полученными в результате постоянного мониторинга событий ИБ, повышая уровень журнализации, использовать рекомендованные меры защиты против известных сетевых атак (эксплойты), резервное копирование информационных ресурсов, готовые антивирусные программные средства для недопущения внедрения вредоносного кода в сеть Электронной библиотеки, использование систем выявления атак, систем

предотвращения вторжений и межсетевого экранирования. Данные требования необходимо оформить в раздел частных политик и описать конкретные решения по защите. Согласно представленным угрозам сформулированы следующие частные политики:

- Антивирусная политика.
- Резервное копирование информационных ресурсов.
- Правила поддержания БД рекомендованных мер защиты против известных сетевых атак (лучшие практики).
- Организация и поддержание IDS-системы.
- Обеспечение системы предотвращения вторжений.

По каждой из частных политик составляется полный список инцидентов и перечень процедур по их обработке.

Для обеспечения целостности структуры веб-сайта должны соблюдаться меры по отношению к отдельному классу сетевых атак типа XSS, для предотвращения которых необходимо создать правила по экранированию входных и выходных данных, использовать только фиксированные типы кодировок, периодически проводить плановый анализ программного кода веб-сайта.

Администратор несет персональную ответственность за нарушение правил пользования АРМ, сервером и сетевым оборудования. Администратор подписывает обязательство о соблюдении и ответственности за нарушения установленных требований. Система управления инцидентами информационной безопасности предусматривает положения, по которым выявляется инцидент по не легитимному доступу к АРМ, серверу и сетевому оборудованию, в частности хищению, физическому изменению оборудования, и проводятся процедуры по его дальнейшей обработке [5].

Типовые действия, выполняемые в рамках процесса управления инцидентами ИБ, включают следующее:

- идентификацию инцидента ИБ (получение информации о нем, его регистрацию, оценку критичности и классификацию инцидента);
- реагирование на инцидент ИБ (идентификация причин его возникновения, изоляция инцидента и подавление причин его возникновения);

- восстановление после инцидента ИБ (оперативное внесение изменений в конфигурации систем, восстановление данных и закрытие инцидента ИБ);
- последующие действия по инциденту ИБ (анализ первопричин возникшего инцидента ИБ, предоставление отчета об инциденте ИБ заинтересованным сторонам) [6].

Перечень событий ИБ, являющихся инцидентами ИБ:

- DDoS атака;
- активность ВПО;
- XSS атака;
- SQL инъекция;
- хищение/порча оборудования;
- НСД к АРМ администратора.

В таблице 2 описаны угрозы и инциденты ИБ.

Таблица 2 – Угрозы и инциденты ИБ.

Актив подвергающийся угрозе	**Нарушаемое свойство актива**	**Угроза**	**Инцидент**
БД	Доступность	Сетевая	DoS/DDoS, активность вредоносного ПО, SQL-инъекция
		НСД к АРМ администратора	Хищение/удаление/изменение информации
	Целостность	Сетевая	Активность вредоносного ПО, SQL-инъекция
		НСД к АРМ администратора	Хищение/удаление/изменение информации
	Конфиденциальность	Сетевая	Активность вредоносного ПО, SQL-инъекция
		НСД к АРМ администратора	Хищение/удаление/изменение информации
Веб-сайт	Доступность	Сетевая	DoS/DDoS, SQL-инъекция, XSS-атака
	Целостность	Сетевая	SQL-инъекция, XSS-атака
	Конфиденциальность	Сетевая	SQL-инъекция, XSS-атака
ПО	Доступность	Сетевая	Активность вредоносного ПО
		НСД к АРМ администратора	Активность вредоносного ПО
	Целостность	Сетевая	Активность вредоносного ПО
		НСД к АРМ администратора	Использование вредоносного ПО
	Конфиденциальность	НСД к АРМ администратора	Активность вредоносного ПО
Оборудование	Доступность	Хищение/порча оборудования	Физические действия злоумышленника
		НСД к АРМ администратора	Аппаратная закладка
	Целостность	Хищение/порча оборудования	Физические действия злоумышленника
		НСД к АРМ администратора	Аппаратная закладка
	Конфиденциальность	Хищение/порча оборудования	Физические действия злоумышленника
		НСД к АРМ администратора	Аппаратная закладка

При возникновении одного из вышеперечисленных инцидентов ИБ: необходимо произвести следующие действия:

1. Идентификация. Установите тип происходящей атаки, определите, какие компоненты инфраструктуры подвержены ее влиянию.

2. Реагирование. Изменение конкретных параметров системы и объектов ее функционирования для предотвращения атаки и минимизации потерь.
3. Восстановление. Убедитесь, что доступность сервисов, на которые было оказано влияние, восстановлена.
4. Последующие действия. Продумайте, какие подготовительные шаги вы можете предпринять, чтобы реагировать на инциденты быстрее и более эффективно [2].

Рассмотрим это на примере инцидента DDoS-атаки.

1.Идентификация.

Установите тип происходящей DDoS-атаки. Определите, являетесь ли вы целью атаки, или воздействие на вас является лишь побочным эффектом, вызванным атакой на другую цель.

Проанализируйте нагрузку и лог-файлы серверов, маршрутизаторов, межсетевых экранов, приложений и других компонентов инфраструктуры, подверженным влиянию атаки.

Определите характеристики трафика DDoS-атаки, отличающиеся от обычного, полезного трафика:

- IP-адреса отправителей пакетов, их провайдеры (подсети) и т.п.
- Номера портов получателя
- Адреса URL
- Флаги протоколов

Уведомите пользователей Электронной библиотеки об атаке.

2.Реагирование.

Если узким местом является отдельная функция приложения, временно отключите эту функцию.

Попытайтесь снизить или заблокировать DDoS-трафик максимально близко к магистральному провайдеру с помощью маршрутизатора, межсетевого экрана, балансировщика нагрузки, специализированных устройств и т.д.

Закройте ненужные соединения или процессы на серверах и маршрутизаторах, внесите изменения в настройки TCP/IP на них.

Настройте фильтр для блокировки трафика, который отправляют ваши системы в ответ на DDoS-трафик, чтобы избежать передачи по сети ненужных пакетов.

Свяжитесь с провайдером, чтобы убедиться, что он принял меры для исправления ситуации.

3.Восстановление.

Убедитесь, что доступность сервисов, на которые было оказано влияние, восстановлена. Убедитесь, что производительность инфраструктуры вернулась на нормальный уровень. Переключите трафик обратно на обычный маршрут. Перезапустите остановленные сервисы.

4.Последующие действия.

Продумайте, какие подготовительные шаги вы можете предпринять, чтобы реагировать на инциденты быстрее и более эффективно. При необходимости внесите изменения в предположения, с учетом которых выполнялись подготовительные шаги в отношении DDoS-атак. Оцените эффективность процесса реагирования на произошедший инцидент, включая работу людей и коммуникаций [7].

Таким образом, в статье рассмотрен пример обеспечения информационной безопасности Электронной библиотеки, а также основные аспекты действий по реагированию в конкретных ситуациях для предотвращения DDoS-атак.

Библиографический список

1. Акофф Р. Планирование будущего корпорации / Р. Акофф. - М.: Сирин, 2002. - 256 с.

2. Герасименко В.А. Основы защиты информации / В.А. Герасименко, А.А. Малюк. - М: ООО "Инко-бук" в ППО "Известия", 1997. - 537с.

3. Девянин П.Н. Модели безопасности компьютерных систем/ П.Н. Девянин. - М.: Издательский центр «Академия», 2005. -144 с.

4. Липаев В.В. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств // В.В. Липаев. - Информационный бюллетень "Jet Info". № 3 (130) /2004.

5. Макарова Ю.В., Русанова М.О., Федякова Н.Н. Облачные вычисления // Ю.В. Макарова, М.О. Русанова, Н.Н. Федякова. - Контентус. 2015. №12(41). С. 142-149. http://elibrary.ru/item.asp?id=25684342 (дата обращения: 20.06.2016).

6. Петров А. Б. Открытые информационные системы. Учебное пособие / А. Б. Петров. - М.: МИРЭА, 2000. -38 с.

7. Петров А.Б. Проектирование информационных систем. Безопасность функционирования. Учебное пособие/ А.Б. Петров. - М.:, МИРЭА, 2008. -132 с.