

Железнов Макар Эдуардович

студент кафедры «Институт сквозных технологий (интеллектуальные медиатехнологии)»
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия

Научный руководитель:

Кадомцев Максим Игоревич

доцент кафедры «Институт сквозных технологий»
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия

Безопасность медиаконтента: методы противодействия кибератакам

Аннотация. Многие компании подверглись хакерским атакам, повлекшим за собой нарушения работы на уровне инфраструктуры. После таких атак украденные личные данные работников и клиентов фирм утекают в сеть и становятся общедоступными. С увеличением числа нападений на данные многие фирмы пересмотрели свою политику в вопросе защиты баз данных – они начали развивать механизмы, способные предотвратить несанкционированный доступ злоумышленников к информации. Проблемой в данной статье является увеличение числа атак в сети и обеспечение безопасности медиаконтента. Целью данной статьи является внедрение и развитие механизмов противодействия угрозам в сети с использованием новых подходов к защите от несанкционированного доступа злоумышленников к базам данных.

Ключевые слова: кибербезопасность, утечка данных, информация, защита данных, злоумышленники, несанкционированный доступ, противодействие атакам на сеть, база данных, защита персональных данных.

Jeleznov Makar Eduardovich

student of the department "Institute of End to-end Technologies (Intelligent Media technologies)"

Don State Technical University

Rostov-on-Don, Russia

Scientific Supervisor:

Kadomcev Maxim Igorevich

Associate Professor of the Department of "Institute of End-to-end Technologies"

Don State Technical University

Rostov-on-Don, Russia

Media content security: methods of countering cyber attacks

Abstract. Many companies have been subjected to hacker attacks, resulting in disruptions at the infrastructure level. After such attacks, the stolen personal data of employees and clients of companies leaks online and becomes publicly available. With the increasing number of attacks on data, many firms have revised their database protection policies – they have begun to develop mechanisms that can prevent unauthorized intruders from accessing information. The problem in this article is the increase in the number of attacks on the network and ensuring the security of media content. The purpose of this article is to introduce and develop mechanisms to counter threats in the network using new approaches to protect against unauthorized access to databases by intruders.

Keywords: cybersecurity, data leakage, information, data protection, intruders, unauthorized access, countering attacks on the network, database, personal data protection.

Количество сетевых атак растет с каждым годом. Многие компании подверглись хакерским атакам, повлекшим за собой нарушения работы на уровне инфраструктуры. После таких атак украденные личные данные работников и клиентов фирм утекают в сеть и становятся общедоступными.

Проблемой в данной статье является увеличение числа атак в сети и обеспечение безопасности медиаконтента. Целью данной статьи является внедрение и развитие механизмов противодействия угрозам в сети с использованием новых подходов к защите от несанкционированного доступа злоумышленников к базам данных.

С увеличением числа нападений на данные многие фирмы пересмотрели свою политику в вопросе защиты баз данных – они начали развивать механизмы, способные предотвратить несанкционированный доступ злоумышленников к информации.

Первой технологией для защиты от несанкционированного доступа злоумышленников являются возможности искусственного интеллекта. На сегодняшний день применение ИИ позволяет реагировать на атаки без каких-либо задержек. Так как сегодня методы работы мошенников дошли до уровня подделки голоса и изображения любого человека, без использования технологий искусственного интеллекта не обезопасить внутренние данные предприятия.[1]

Работа нейросети по защите от подделок голоса и изображения организуется следующим образом: нейросеть обучается на определенном наборе данных, с помощью чего наиболее точно определяет подлинность видеоматериала, анализируя аудио- и видеозапись по огромному числу параметров.

Второй технологией является концепция нулевого доверия. По данной концепции любой пользователь, посетивший страницу, ставится под подозрение. Доступ ко всем данным предоставляется только после тщательной проверки.

Третьей технологией являются облачные сервисы. Многие компании должны перейти на использование облачных технологий. Данные технологии используются для создания, хранения и обработки информации на специализированной облачной платформе.

Четвертой технологией является концепция противодействия «человеческому фактору». Одной из главных причин утечек данных является неумышленное действие работников: открытие ссылок для доступа к информации компании. Необходимо внедрять программы для обучения персонала правильной работе с базами данных. [2]

На сегодняшний день персональные данные стали ценным ресурсом, к которому компания должна подойти с большей ответственностью. За утечку персональных данных предусмотрен штраф до 15 млн.руб. Это стимулирует многие компании больше денежных средств затрачивать на защиту информации и создавать благоприятную среду для работы с персональными данными.



Рисунок 1 – Технологические процессы для защиты персональных данных на предприятии

На рисунке 1 приведены технологические решения для защиты персональных данных, которые включают в себя:

1. Разработка технического задания на систему защиты персональных данных;
2. Разработка технического проекта;
3. Внедрение системы защиты персональных данных;
4. Аттестационные испытания;
5. Консультационная поддержка и сопровождение;
6. Аудит на соответствие требованиям по защите информации;
7. Разработка модели угроз и нарушителя;
8. Разработка организационно-распорядительной документации.

Другой технологией является концепция «недопустимых событий». При фиксировании факта кибератак, деятельность компании блокируется, следовательно, доступ к серверам прекращается и утечка данных не происходит. [3]

В любой компании должна быть организована группа для работы с защитой данных, которая должна состоять из руководителя, операционных менеджеров и специалистов по защите информации. Должен быть разработан сценарий работы при атаках на сеть, который должен состоять из следующих пунктов:

1. Проведение анализа базы данных на утечку информации;
2. При подтверждении утечки оценивается масштаб краденных данных;
3. Оперативное принятие решения по ликвидации причин утечек данных;
4. Предупреждение о происшествии граждан, чьи персональные данные были украдены.

Таким образом, с повышением ответственности персонала и администрации к защите персональных данных и внедрением инноваций, рассмотренных в данной статье, можно достичь высоких показателей в сфере кибербезопасности данных в сети.

Список источников

1. Смит, Дж. и др. (2021). "Тенденции в области киберугроз и безопасности данных". Журнал кибербезопасности, 15 (3), С.211-228;
2. Чен, Л. (2020). "Методы шифрования и защита данных". Международный

журнал информационной безопасности, 25 (4), С.332-349;

3. Браун А. и др. (2019). "Технологии и инструменты кибербезопасности".
Обзор системы безопасности, 14(2), С.87-104.