

Доклад по дисциплине «Основы российской государственности» на тему «Кибербезопасность»

**Работа выполнена
студентами 1
курса 1
факультета, гр.
1101 Вахитовой
Алией**

Казань, 2023

Г

Оглавление

- Введение
- Основная часть:
 1. Раздел 1 - Основные черты российского мировоззрения
 2. Раздел 2 - Государственные решения в области мировоззрения: влияние на общество и культуру
 3. Раздел 3 - Роль государственных решений в формировании мировоззрения общества
 4. Раздел 4 - Влияние государства на формирование ценностей
 5. Раздел 5 - Государственная политика в области мировоззрения
- Заключение

е

Развитие цифровых технологий привело к появлению большого количества цифровых угроз в интернете. Например, кража персональных данных пользователей или атаки хакеров на информационные системы компании с целью вывести их из строя.

В ответ на угрозы появилась область знаний, которая занимается разработкой и внедрением технологий защиты информационных систем от них, — кибербезопасность. Специалисты по кибербезопасности изучают преступления и угрозы в цифровой среде и разрабатывают способы противостоять им. Например, ищут уязвимости в корпоративных системах и совершенствуют протоколы шифрования персональных данных пользователей.

Раздел 1 -

Кибербезопасность — раздел информационной безопасности, в котором изучают процессы формирования, функционирования и эволюции киберобъектов, для выявления источников киберопасности, образующихся при этом, определение их характеристик, а также их классификацию и формирование нормативных документов, выполнение которых должно гарантировать защиту киберобъектов от всех выявленных и изученных источников киберопасности. Также: набор процессов, передовых практик и технологий, которые помогают защитить критически важные системы и сети от цифровых атак.

Цели

- Обеспечить безопасность сетей, устройств и ПО

- Защитить информацию

- Обнаружить угрозы и реагировать на инциденты

- Обучать пользователей



Виды угроз

Угрозы кибербезопасности — это действия злоумышленников, которые они совершают с помощью интернета и программных средств. Перечислим основные виды:

✗ Вредоносное ПО

- Вирусы
- Троянцы, или троянские программы
- Шпионские программы
- Программы-вымогатели

✗ Фишинг (человек переходит по ссылке)

✗ «Человек посередине» (злоумышленник перехватывает



Как защититься от кибератак

Противостоять киберугрозам помогают технологии защиты информации, например антивирусные программы, криптографические методы шифрования данных, брандмауэры и программы для выявления подозрительной активности вроде EDR и IDS-систем.

Пользователи могут защитить свои персональные данные от киберугроз в сети интернет, если будут соблюдать правила кибербезопасности. Перечислим основные:

- Использовать разные и сложные пароли для аккаунтов и устройств. Сложными считаются пароли, которые состоят из букв, цифр и знаков препинания. Их тяжело угадать, а подбирать — долго.
- Включить двухфакторную аутентификацию для доступа к аккаунтам.
- Использовать лицензионные антивирусные программы и регулярно запускать сканирование устройства.
- Не переходить по подозрительным ссылкам на веб-страницах и не скачивать файлы из непроверенных интернет-ресурсов, электронных писем или сообщений в мессенджере от незнакомых отправителей.
- Не переходить по ссылкам из SMS-сообщений, которые пришли без запроса. Например, SMS-сообщение со ссылкой для восстановления доступа к аккаунту на сайте или соцсети.
- Проверять адрес отправителя электронного письма, прежде чем переходить по ссылкам из него, чтобы не стать жертвой фишинга.
- [Использовать VPN](#) при подключении к Wi-Fi сети в общественных местах вроде кафе и поездов.
- Отключать Bluetooth, когда он не используется. Не принимать запросы на подключение от незнакомых людей.
- Настроить резервное копирование данных, чтобы восстановить их в случае пропажи.
- Не игнорировать доступные обновления систем и браузеров. В них обычно исправляют обнаруженные проблемы кибербезопасности.

Дайджест киберинцидентов за ноябрь

Кибератаки

В официальном магазине приложений Xiaomi нашли поддельный клиент Telegram. Его установок настолько много, что фейк занял первое место по популярности в категории «Связь». Версия этого клиента 9.6.9, и отличается от настоящего приложения тем, что показывает уведомления с призами и другими бонусами для пользователя, чтобы украсть его данные.



Telegram

Telegram FZ-LLC



#1 Связь

5.0★
Более 100
отзывов

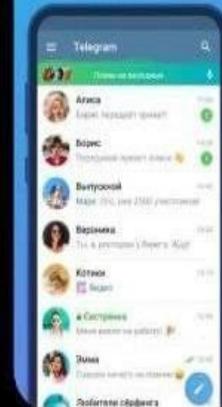
Более 12 млн.
Загрузки

57,7 МБ

Открыть

Скорость

Быстрый и легкий обмен сообщениями.



Функциональность

Неограниченный размер групповых чатов и звонков.



Безопасность

Надежное шифрование всех сообщений и звонков.



Приватность

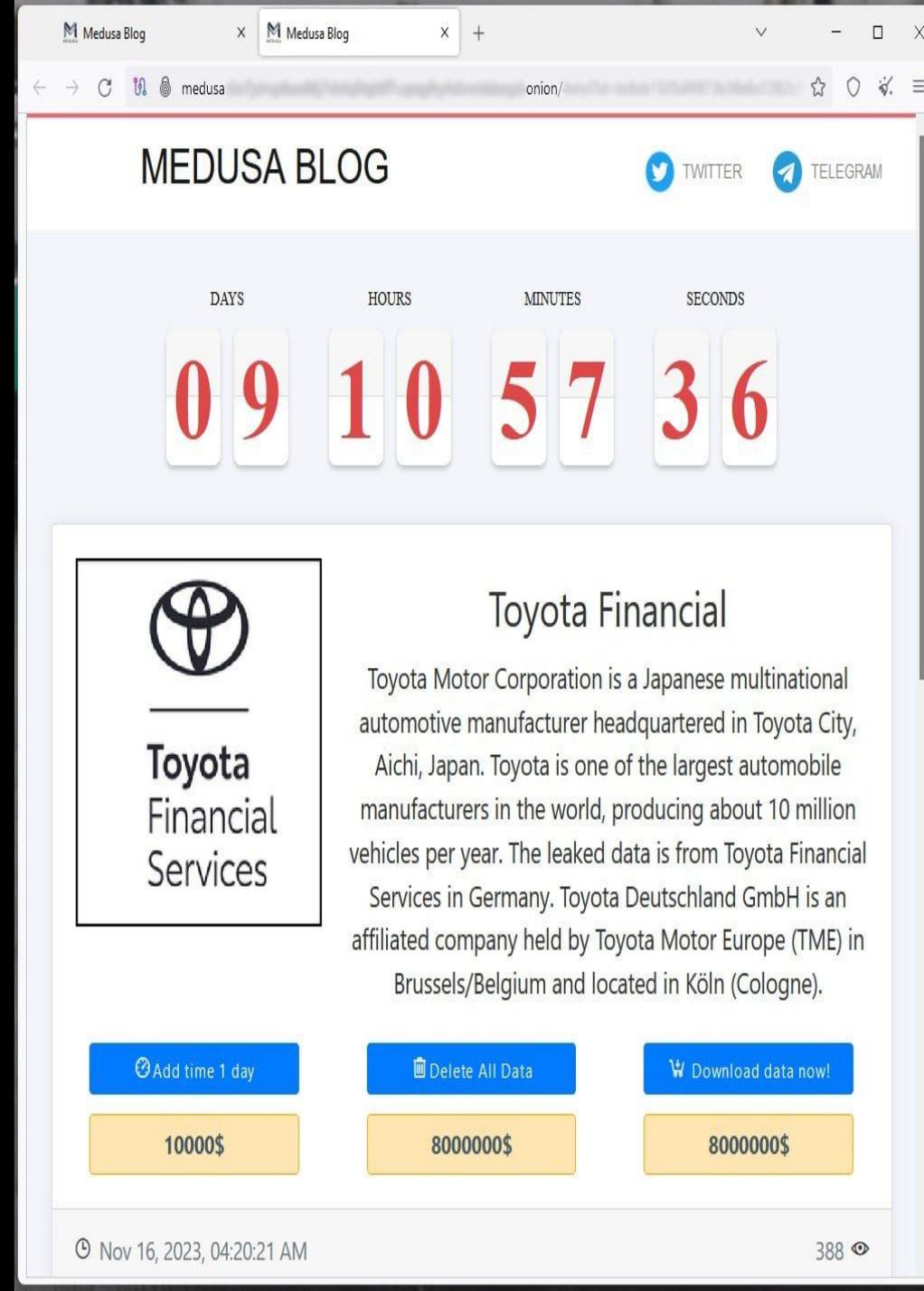
Недоступность для...



Компания Toyota Financial Services (TFS), дочерняя компания Toyota Motor Corporation, обнаружила несанкционированный доступ к своим системам в Европе и Африке. Одновременно с этим хак-группа Medusa внесла компанию в список своих жертв, потребовав 8 000 000 долларов выкупа за удаление якобы украденных данных.

Toyota Financial Services является международной компанией, которая присутствует на 90% рынков, где Toyota продает свои автомобили и предоставляет своим клиентам услуги автокредитования.

Большинство документов написано на немецком языке, то есть, похоже, хакерам удалось получить доступ к системам европейских подразделений Toyota.



The screenshot shows a ransomware payment page titled "MEDUSA BLOG". At the top, there are social media links for Twitter and Telegram. Below the title is a countdown timer showing 09 days, 10 hours, 57 minutes, and 36 seconds. The main content area features the Toyota Financial Services logo and a description of the company. Below the description are three buttons: "Add time 1 day" (10000\$), "Delete All Data" (8000000\$), and "Download data now!" (8000000\$). The page footer shows the date and time: "Nov 16, 2023, 04:20:21 AM" and a view count of "388".

MEDUSA BLOG

TWITTER TELEGRAM

DAYS HOURS MINUTES SECONDS

09 10 57 36

 Toyota Financial Services

Toyota Financial

Toyota Motor Corporation is a Japanese multinational automotive manufacturer headquartered in Toyota City, Aichi, Japan. Toyota is one of the largest automobile manufacturers in the world, producing about 10 million vehicles per year. The leaked data is from Toyota Financial Services in Germany. Toyota Deutschland GmbH is an affiliated company held by Toyota Motor Europe (TME) in Brussels/Belgium and located in Köln (Cologne).

Add time 1 day 10000\$

Delete All Data 8000000\$

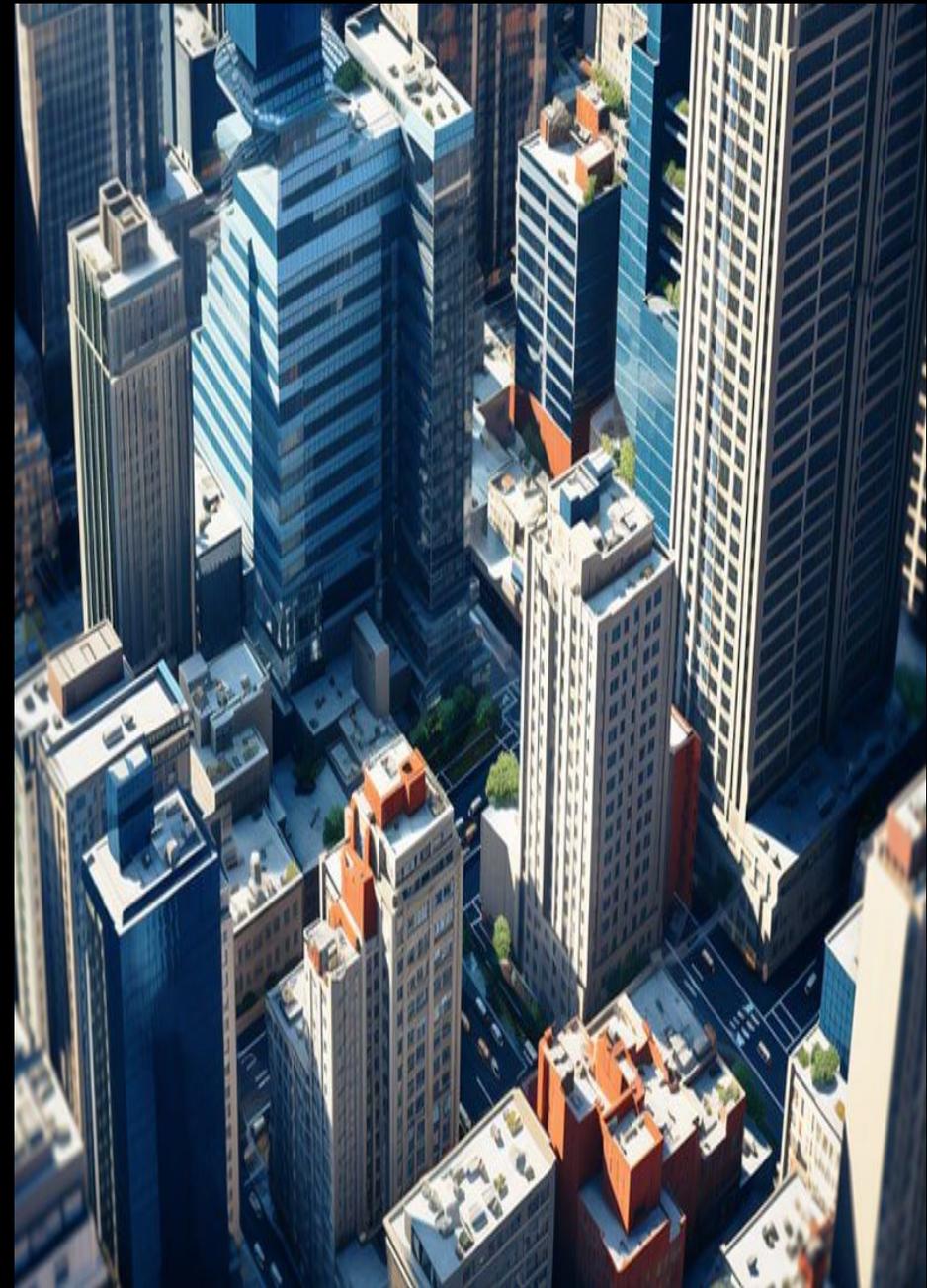
Download data now! 8000000\$

Nov 16, 2023, 04:20:21 AM 388

Кибератака парализовала рынок недвижимости США.

В США кибератака парализовала рынок недвижимости. Хакеры взломали крупнейшего страховщика FNF, из-за чего пришлось отключить ряд систем, которые задействованы в страховании недвижимости. А без него проводить сделки не представляется возможным.

Ответственность за атаку взяла на себя группа ALPHV/BlackCat 22 ноября, однако детали атаки пока не раскрываются. Группа BlackCat опубликовала сообщение, в котором раскритиковала специалистов по реагированию на инциденты Mandiant за их бездействие в отношении атаки. Группа также объявила о том, что даст компании FNF дополнительное время для связи с вымогателями перед раскрытием дополнительной



На одном из теневых форумов на продажу выложили данные 815 миллионов граждан Индии. Лот содержит 1.8 Тб информации, а просят за него \$80 тыс.

Aadhaar - это ничем необычный идентификатор, обладающий биометрическими данными, который выдается гражданам Индии и иностранным гражданам, проживающим там постоянно. Его основное назначение - облегчить финансовые транзакции и обеспечить безопасность граждан. Однако, ситуация в корне изменилась, и далеко не в лучшую сторону.

Очевидно, что инцидент с утечкой персональных данных Aadhaar стал еще одним напоминанием о необходимости более строго контролировать доступ к ценным данным. Каждый гражданин должен принять меры по защите своей конфиденциальности и следить за тем, чтобы его данные не попали в руки



УК РФ Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

[Статья 272. Неправомерный доступ к компьютерной информации](#)

[Статья 273. Создание, использование и распространение вредоносных компьютерных программ](#)

[Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей](#)

[Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации](#)

[Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования](#)

**Заключен
ие**

The background is a complex, abstract digital landscape. It features a dense network of blue lines and data points, creating a sense of depth and movement. The lines are arranged in various patterns, some forming grids and others appearing as flowing streams. The overall color palette is dominated by shades of blue, ranging from light, airy tones to deeper, more saturated blues. The perspective is from a high angle, looking down into the digital structure, which adds to the futuristic and technological feel of the image.

**Спасибо за
внимание!**