58. ВРЕДОНОСНЫЕ МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ И СПОСОБЫ ЗАЩИТЫ ОТ НИХ

Граськова С.И., студент гр.473904, Федюкович Т.В., ассист. каф. ЭИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ефремов А.А. – канд. экон. наук, доцент каф. ЭИ

Аннотация. В последнее время наблюдается рост числа вредоносных мобильных приложений, это связано с различными факторами, включая распространение смартфонов, недостаточная защищенность мобильных операционных систем. В данной работе рассматриваются причины появления вредоносных приложений, проблемы, связанные с этим, классификация, распространенные мифы в которые верят люди и методы защиты от подобных угроз. Особое внимание в работе уделено социальным и практическим аспектам. На основе проведенного анализа предложены были предложены рекомендации по повышению уровня безопасности мобильных приложений и защите персональных данных пользователей.

Ключевые слова. Вредоносные приложения, киберугрозы, фишинговые ссылки, трояны, spyware, adware, APK-файлы, удаленный доступ, цифровая гигиена, сталкерское ПО, backdoor, антивирус, ИИ.

Гаджеты уже достаточно давно всячески упрощают нашу жизнь, однако всегда есть риск установить на свое устройство вредоносное приложение.

Повсеместное распространение смартфонов в повседневной жизни сделало их целью для злоумышленников, стремящихся получить доступ к пользовательским данным и нарушить работу устройств. Обнаружение вредоносного ПО на Android стало необходимым для защиты конфиденциальности пользователей и целостности устройств. Еще в 2014 году лишь около 1 млрд человек пользовались смартфонами, а к 2024 году их количество превысило 4 млрд. Следующая причина — это отсутствие глубоких знаний в области кибербезопасности из-за чего пользователи скачивают приложения из ненадежных источников. Также отсутствует глобальный контроль за киберугрозами. Современные вредоносные программы становятся все более приспособленными, используя методы обхода защитных приложений. Это все приводит к нижеперечисленным результатам.

1. Частые случаи взломов и утечек данных сильно подрывают доверие пользователей к мобильным сервисам. Киберпреступления наносят вред как отдельным индивидам, так и компаниям. Кража финансовых данных приведет не только к денежным потерям, а еще к потере репутации и дальнейшем ее восстановлении, которое потребует дополнительных затрат.

2. Вирусы приводят к замедлению и сбоям в работе устройства. Вредоносное ПО использует данные смартфона для своих нужд. Например, вирус майнер может незаметно перегревать устройство и истощать батарею.

3. Возникают трудности удаления и восстановления системы. Некоторые вирусы получают root-доступ или интегрируются в системные процессы. После чего от них можно избавиться только с помощью сброса до заводских настроек или даже в некоторых ситуациях только после перепрошивки устройства, что ведет к потери данных.

4. Распространение вредоносных мобильных приложений оказывает серьёзное влияние не только на пользователей, но и на экономику в целом. По оценкам международной аналитической компании Cybersecurity Ventures, ежегодные мировые убытки от киберпреступности, включая атаки через мобильные устройства, к 2024 году превысили 10 трлн долларов США, и эта цифра продолжает расти. Только вредоносное ПО для Android стало причиной ущерба в десятки миллиардов долларов в год, в том числе из-за кражи финансовых данных, вымогательства и мошенничества. В России, по данным «Лаборатории Касперского», в 2023 году зафиксировано более 1,5 млн атак с использованием мобильных вирусов, а общие потери пользователей оцениваются в миллиарды рублей.

Мобильные атаки особенно опасны тем, что затраты на восстановление после инцидента значительно превышают стоимость профилактики. В условиях активной цифровизации и зависимости от смартфонов, вредоносные приложения стали не просто неудобством, а серьёзной угрозой национальной и глобальной цифровой экономике.

Безопасность устройств Apple или Android начинается с приложений. Приложения запрашивают разрешение на доступ к данным, которые им нужны для корректной работы. Если при этом предоставить лишние разрешения, они могут воспользоваться ими в свою пользу. Также и подключение к общедоступным сетям ставит под угрозу безопасность мобильного телефона. В связи с тем, что такие подключения незащищены, есть риск перехвата соединения и получение доступа к

данным в режиме реального времени. Мошенники могут без ведома пользователя установить на устройство вредоносное ПО, что позволит им следить за всеми действиями.

Далее рассмотрим классификацию вредоносных мобильных приложений в таблице 1.

Таблица 1 – Классификация вредоносных мобильных приложений.

Критерий	Тип	Описание
По способу распространения	SMS/фишинговые ссылки	Скачивание ПО через вредоносные ссылки
	Официальные и неофициальные магазины	Вредоносные приложение, размещенные в маркетах
	Сторонние APK-файлы	Установка приложений из ненадежных источников
По цели атаки	Слежка	Наблюдение за действиями пользователя
	Кража персональных данных	Доступ к личным и финансовым данным
	Полный контроль устройства	Захват устройства с целью удаленного управления
	Нарушение работы устройства	Удаление файлов, замедление работы устройства, перегрев
По типу действия	Trojan (трояны)	Маскировка под легальные приложения
	Spyware	Слежка за пользователем
	Adware	Реклама без согласия пользователя
	Backdoor	Создание скрытого доступа к управлению

После ознакомления с классификацией вредоносных приложений перейдем к основным методам защиты от них и популярным заблуждениям. Безопасность мобильных устройств включает в себя ряд аспектов, начиная с правил безопасности использования устройств и заканчивая приложениями и продуктами с функциями защиты.

Первое заблуждение о том, что в официальных магазинах приложений не бывает мошеннических программ. В магазинах вроде Google Play и App Store действительно есть фильтры безопасности. И, как правило, туда попадают только проверенные программы. Разработчики подписывают договор с площадкой, по которому они, к примеру, обязуются не рассылать спам, тайно не собирать данные пользователей, не дезинформировать их. Однако бывает, что после того, как набрав аудиторию, разработчики начинают нарушать правила. Магазины не всегда успевают отследить нарушения.

В любом случае стоит выбирать приложения в официальных магазинах, там риск ниже, но стоит обратить внимание на количество скачиваний, рейтинг приложения и свежие комментарии пользователей.

Следующее популярное заблуждение связано с антивирусом. Принято считать, что он защитит от всех проблем. Одна из главных причин уязвимости устройств, от которой не спасет никакой антивирус, — это ошибки самого пользователя. Например, установленная программа обладает большими правами, чем антивирус: она его отключит и продолжит работать.

Для решения данной ситуации стоит регулярно обновлять ПО и антивирусы, не переходить на ссылки от незнакомцев.

Третье заблуждение о том, что безопасное приложение никогда не запрашивает доступ к личным данным. Всем приложениям необходим доступ к различным функциям и информации, однако стоит всегда обращать внимание на то, какие данные запрашивает приложение. Соглашаться только если в этих данных действительно есть необходимость.

Нужно выбирать сложные пароли. Пароль должен состоять не менее чем из 8 символов: цифр, строчных и заглавных букв, специальных символов. Лучше не использовать популярные слова и общеизвестные сокращения. Не стоит использовать даты рождения, имена и фамилии. Пароли должны быть разными для каждого аккаунта. Каждый раз вводите пароль заново вручную — не сохраняйте его для автоматического ввода. Стоит настроить двойную идентификацию.

Регулярно нужно создавать резервные копии данных. Это поможет быстрее восстановить данные с потерянного или украденного телефона и перенести их на новый.

С развитием технологий искусственный интеллект (ИИ) начал играть ключевую роль в сфере кибербезопасности, в том числе и в защите мобильных устройств. Современные антивирусные решения используют алгоритмы машинного обучения для анализа поведения приложений, выявления

подозрительной активности и обнаружения угроз, даже если они ранее не были занесены в базы данных.

Например, такие решения, как Kaspersky Mobile Security, ESET Mobile Security и Bitdefender применяют поведенческий анализ на основе ИИ, чтобы выявлять вредоносные действия — перехват СМС, скрытая передача данных, несанкционированный доступ к камере или микрофону. Технология Google Play Protect (рисунок 1), встроенная в Android, также использует ИИ для ежедневной проверки миллиарда установленных приложений, выявляя вредоносные действия даже в программах, которые изначально прошли модерацию.

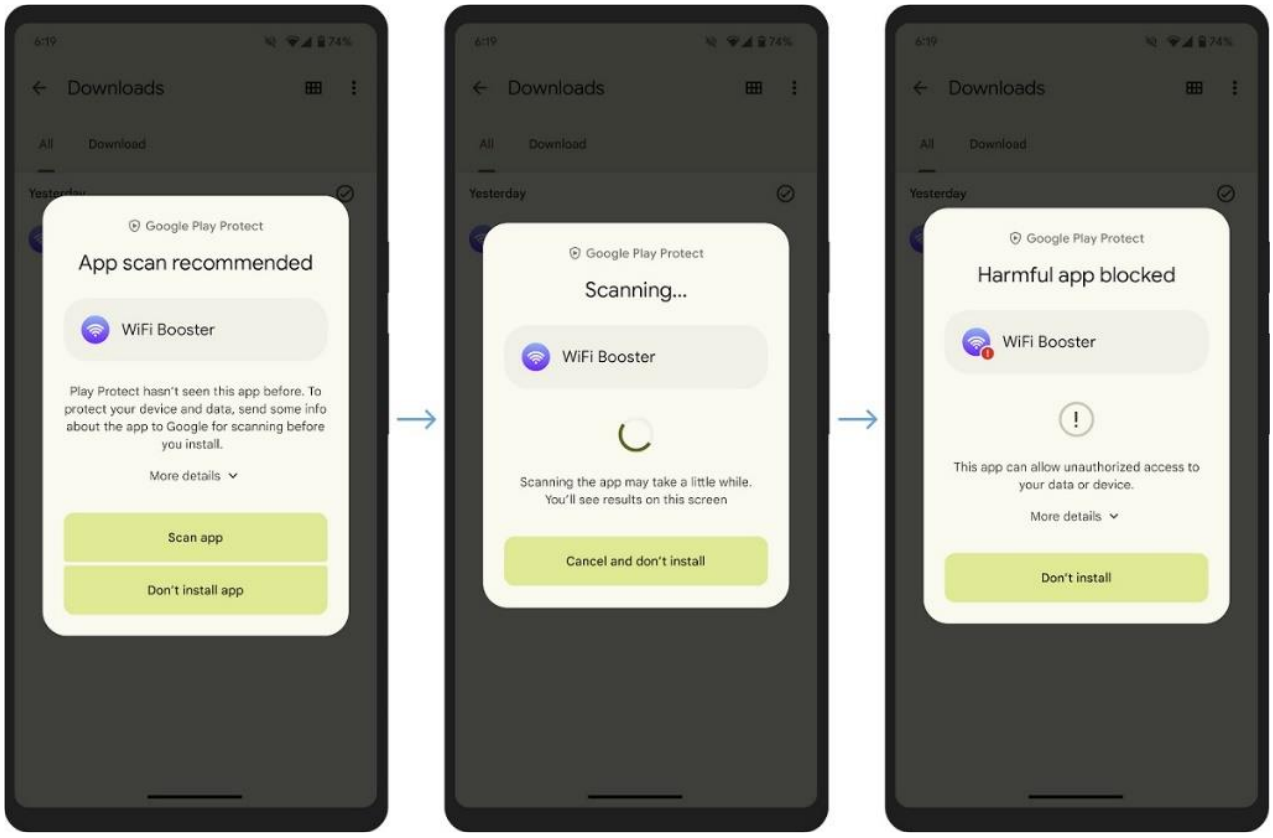

Рисунок 1 – Функция Live Threat Detection от Google

ИИ способен распознавать вредоносные шаблоны, выявлять скрытую активность и предотвращать атаки в реальном времени. Благодаря этому защита становится более гибкой и оперативной — без необходимости ручного обновления антивирусных баз.

Однако важно понимать, что те же технологии начинают использовать и злоумышленники: с помощью нейросетей создаются фальшивые приложения, генерируются тексты фишинговых сообщений, имитирующих стиль реальных компаний.

Таким образом, ИИ стал не только инструментом защиты, но и частью цифровой гонки между разработчиками систем безопасности и создателями угроз. Главная задача сегодня — обеспечить, чтобы технологии работали на благо пользователей, а не против них.

Современные угрозы, связанные с вредоносными мобильными приложениями, требуют не только технических решений, но и системного подхода к профилактике через образование. Как уже было сказано ранее, недостаток знаний в области информационной безопасности остаётся одной из ключевых причин уязвимости пользователей. Образовательные программы, направленные на формирование навыков безопасного поведения в цифровой среде, становятся приоритетным направлением как на уровне государства, так и внутри коммерческих организаций. Особое внимание следует уделять обучению основам кибергигиены: анализу источников приложений, проверке разрешений, распознаванию фишинговых атак и работе с резервными копиями. Практика показывает, что даже базовая осведомлённость позволяет значительно снизить риски заражения вредоносным ПО. Внедрение образовательных модулей по кибербезопасности в систему школьного и высшего образования, а также проведение массовых информационных кампаний среди населения являются неотъемлемыми элементами комплексной защиты цифровой инфраструктуры.

Уже сегодня многие школы и вузы начинают внедрять курсы по информационной безопасности, где обучают, как распознавать фишинг, правильно выбирать источники для загрузки приложений и управлять разрешениями. Кроме того, многие компании проводят внутренние тренинги для сотрудников, ведь от действий каждого пользователя зависит безопасность всей информационной системы.

Вредоносные мобильные приложения представляют собой серьёзную угрозу как для частных пользователей, так и для организаций. Их распространение напрямую связано с ростом использования мобильных устройств, отсутствием должной осведомлённости пользователей и недостаточной защитой со стороны разработчиков. Киберпреступники всё более изощрённо используют уязвимости операционных систем и слабости в безопасности приложений для получения доступа к личной и финансовой информации, а также для вредоносных действий, таких как слежка и заражение устройств.

Тем не менее, современная кибербезопасность активно развивает инструменты защиты, включая искусственный интеллект для анализа поведения приложений, а также внедряет образовательные программы для повышения цифровой грамотности населения. Эти меры, в сочетании с правильными привычками пользователей и использованием надёжных средств защиты, могут существенно снизить риски заражения вредоносным ПО. Важно, чтобы профилактические мероприятия стали частью повседневной культуры, а также чтобы пользователи осознавали свою ответственность за сохранность личных данных.

Таким образом, эффективная защита от мобильных угроз требует комплексного подхода, включающего как технические средства, так и образование, а также ответственное отношение пользователей к своей безопасности в цифровом мире.

Список использованных источников:

1. Improving mobile security: A study on android malware detection using LOFF [Электронный ресурс] – Режим доступа: https://sciendo.com/article/10.2478/ijmce-2025-0018, свободный.

2. Безопасность мобильных устройств: преимущества, перечень угроз и полезные рекомендации [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-mobile-security, свободный.

3. Мифы и правда о безопасности мобильных приложений [Электронный ресурс] – Режим доступа: https://fincult.info/article/mify-i-pravda-o-bezopasnosti-mobilnykh-prilozheniy/?ut, свободный.

MALWARE MOBILE APPS AND WAYS TO PROTECT YOU FROM THEM

Graskova S.I., student gr.473904, Fedziukovich T.V., Assistant of the Department of EI

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Efremov A.A. – Candidate of Economic Sciences, Associate Professor

Annotation. Recently, there has been an increase in the number of malicious mobile applications, this is due to various factors, including the spread of smartphones, insufficient security of mobile operating systems. This paper examines the causes of the emergence of malicious applications, the problems associated with this, classification, common myths that people believe in and methods of protection against such threats. Particular attention in the work is paid to social and practical aspects. Based on the analysis, recommendations were proposed to improve the security level of mobile applications and protect users' personal data.

Keywords. Malicious applications, cyber threats, phishing links, trojans, spyware, adware, APK files, remote access, digital hygiene, stalker ware, backdoor, antivirus, AI.