ПОДХОДЫ К МАТЕМАТИЧЕСКОМУ МОДЕЛИРОВАНИЮ КИБЕРАТАК НА МОБИЛЬНЫЕ УСТРОЙСТВА

Михайлов Д.М.[1], Дворянкин С.В.[2], Чуманская В.В.[3]

Аннотация

Актуальность тематики защиты мобильных устройств от кибератак обусловлена существенным ростом количества и доли мобильных гаджетов среди современных устройств доступа в сеть Интернет.

***Цель статьи** заключается в математическом обосновании и формализации моделей наиболее распространенных атак на мобильные устройства. На основе построенных моделей предлагаются способы предотвращения и нейтрализации вторжений в систему смартфонов и планшетных компьютеров.*

***Методы:** прикладной системный анализ результатов обобщения и классификации типовых видов атак на мобильные устройства, элементы теории вероятности.*

***Результаты**: определены особенности механизмов формирования уязвимостей мобильных устройств. Выявлены важные аспекты определения эффективности современных технологий защиты от кибератак на мобильные устройства. Дан краткий обзор основных подходов к математическому моделированию самых распространенных атак. Сформулированы дополнительные требования по адекватному выбору методов защиты в зависимости от вида атак. Сформулированы рекомендации по обеспечению безопасности мобильного устройства от возможной угрозы. Предложены методы снижения вероятности поражения системы путем наиболее распространённых атак.*

***Ключевые слова:** смартфон, планшет, цифровая экономика, цифровая инфраструктура, перебор паролей, программы-эксплоиты, аппаратные и программные закладки, методы защиты от атак, организационные меры защиты, технические меры защиты, выяснение уязвимостей.*

DOI:10.21681/2311-3456-2021-6-62-67

Введение

Одной из основных тенденций цифровой экономики является увеличение доли смартфонов и планшетных компьютеров по отношению к традиционным персональным компьютерам. По относительным показателям роста производительности смартфоны опережают компьютеры. По данным консалтингового агентства Gartner во втором квартале

2021 года мировые поставки смартфонов достигли 328 млн штук, в то время как поставки персональных компьютеров за аналогичный период насчитывают порядка 80 млн штук[4,5]. Нарастающий тренд поставок смартфонов отмечает также и International Data Corporation, прогнозируя рост в 2021 году на уровне десяти процентов[6,7].

Смартфон, как и персональный компьютер (ПК), работает под управлением операционной системы (ОС), которая по своему принципу построения и работы во многом аналогична распространенным ОС для ПК. При этом смартфоны хранят и обрабатывают оперативно значимые данные, под которыми в работе понимаются данные, которые имеют ценность для владельца в течение определенного времени, после которого их важностью можно пренебречь.

4 Press release “Gartner Says Worldwide Smartphone Sales Grew 26% in First Quarter of 2021” 07.06.2021// GARTNER.COM: Gartner consulting agency’s website. URL: https://www.gartner.com/en/newsroom/press-releases/2021-06-07-1q21-smartphone-market-share (date of last request 14.10.2021)

5 Пресс-релиз “Gartner Says Worldwide Smartphone Sales Grew 10.8% in Second Quarter of 2021” от 01.09.2021// GARTNER.COM: сайт консалтингового агентства Gartner. URL: https://www.gartner.com/en/newsroom/press-releases/2021-09-01-2q21-smartphone-market-share ((date of last request 14.10.2021)

6 Press release “PC Demand Remained Strong in the Second Quarter Amid Early Signs That Market Conditions May Be Cooling, According to IDC” от 12.07.2021// IDC.COM: International Data Corporation’s website. URL: https://www.idc.com/getdoc.jsp?containerId=prUS48069721 (date of last request 14.10.2021)

7 Press release “Global Smartphone Shipments Continue to Grow Led by Strong Recovery in Many Emerging Markets, According to IDC” от 30.08.2021// IDC.COM International Data Corporation’s website. URL: https://www.idc.com/getdoc.jsp?containerId=prUS48194821 (date of last request 14.10.2021)

1 Михайлов Дмитрий Михайлович, кандидат технических наук, эксперт Китайского филиала Института БРИКС по изучению сетей будущего, Шэньчжэнь, Китай.E-mail: mikhaylovdm@bifnc.cn

2 Дворянкин Сергей Владимирович, доктор технических наук, профессор, главный научный сотрудник Института информационных наук Московского государственного лингвистического университета, г. Москва, Россия. E-mail: DvoryankinS@linguanet.ru

3 Чуманская Вера Васильевна, аспирант Федерального государственного бюджетного научного учреждения «Национальный исследовательский институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук», Москва, Россия. Email: vera.chumanskaya@gmail.com. ORCID: 0000-0002-8335-2751

Современные исследования говорят о том, что с каждым годом количество кибератак на мобильные устройства, к которым относятся смартфоны, увеличивается [1-3]. Выбор эффективного средства защиты от таких атак напрямую зависит от понимания того, какие методы, программные и аппаратные средства были использованы при атаке [4-10].

При разработке средств предотвращения атак на мобильные устройства следует опираться на математические модели самых распространённых атак.

Базовые модели атак на мобильные устройства

Приведем некоторые модели самых распространенных атак согласно отчету Check Point Software's Mobile Security Report 2021[8]. Важно отметить, что разбираемые атаки являются базовыми. Под базовыми атаками в данной статье мы понимаем те атаки, к которым сводятся все возможное множество атак на мобильные устройства.

Базовыми атаками являются:

1. *Атаки с использованием метода перебора паролей;*
2. *Атаки с использованием вредоносных программ-эксплоитов;*
3. *Атаки с использованием дополнительного оборудования;*
4. *Атаки с использованием аппаратных и программных закладок.*

Разберем поочередно каждую из атак.

Атаки с использованием метода перебора паролей

Атака методом подбора пароля является одним из наиболее распространенных методов получения несанкционированного доступа к данным для любой информационной системы, содержащей аутентификацию по паре имя пользователя-пароль в своем периметре безопасности. Это связано, в основном, с тем, что практически любая атака (исключение составляют программные и аппаратные закладки) рано или поздно останавливается на уровне системы аутентификации (будь то система аутентификации Wi-Fi или встроенная в ОС аутентификация при получении привилегий). Атака методом перебора пароля имеет место при попытке получения несанкционированного доступа как для телефонных аппаратов абонентов, так и для элементов инфраструктуры сотовых систем подвижной связи (ССПС).

Как правило, подбор пароля методом перебора позволяет получить доступ в 100% случаев, однако продолжительность атаки, определяемая общим числом комбинаций и скоростью перебора, может занимать значительное время даже при небольшой длине пароля в 5-10 символов.

Считая пароли равновероятными, возможно составить функцию атаки $f_{П}(t,X)$, в основе которой лежит метод подбора паролей к программному обеспечению объекта атаки - X.

Таким образом, $f_{П}(t,X)$ – функция, значение которой равно вероятности того, что пароль будет найден за время t.

$$f_{П}(t,X)=\frac{v}{N_1}*t,\ t\in\left[0;\frac{N_1}{v}\right], \quad (1)$$

где N_1 – общее количество комбинаций, v – скорость проверки комбинаций.

Наряду с полным перебором существуют также словари наиболее часто используемых паролей. Эти словари составляются на основе статистических данных о наиболее часто используемых паролях и дают среднюю эффективность, по различным оценкам, 10-25% [10]. Принимая вероятность нахождения пароля в словаре за переменную величину a, получим

$$f_{П}(t,X)=a*\frac{v}{N_2}*t,\ t\in\left[0;\frac{N_2}{v}\right], \quad (2)$$

где N_2 – количество паролей в словаре.

Рассмотрим теперь применение существующих методов защиты от атак подбором пароля. С точки зрения подхода, эти методы можно свести к:

- организационным методам – введению парольной политики;
- техническим методам – введению обязательных временных промежутков между попытками аутентификации.

С точки зрения представления функции распределения вероятностей подбора пароля, методы вносят следующие поправки в формулу:

- скорость подбора пароля v становится функцией времени (либо константой, зависящей не только от скорости канала связи, но и от системных настроек);
- накладывается ограничение на минимальную длину пароля, и, как следствие, на минимальное значение общего количества комбинаций N_1;
- применение политики регулярной смены пароля периодически «сбрасывает» вероятность при атаке перебором;
- проверка пароля на стойкость исключает возможность словарной атаки, поскольку корректно реализованный механизм проверки стойкости также использует поиск потенциального пароля по словарю.

Таким образом, в общем случае при введении организационных и технических мер по защите системы аутентификации от атак подбором пароля остается единственная возможность подобрать пароль полным перебором. Тогда функция распределения вероятностей принимает вид

$$f_{П}(t,X)=\frac{v(t)}{N_1}*t,\ t\in\left[0;\min\left(\frac{N_1}{v};\ T_{\text{смены пароля}}\right)\right], \quad (3)$$

где $T_{\text{смены пароля}}$ – период обязательной смены пароля.

Атака с использованием вредоносных программ-эксплоитов

Получение несанкционированного доступа методом применения программ-эксплоитов является вторым по распространенности типом атак на цифровую инфра-

8 Analytical report of Check Point Software LTD "Mobile Security Report 2021" 12.04.2021// CHECKPOINT.COM. URL: https://resources.checkpoint.com/cyber-security-resources/mobile-security-report-2021 (date of last request 14.10.2021)

структуру ССПС при преодолении периметра защиты.

Эксплоиты – это единственный способ быстрого получения возможности выполнения удаленного кода и повышения привилегий, однако эксплоиты в большинстве своем являются узконаправленными на определенные типы ОС и сервисного программного обеспечения, выполняемого в их рамках.

Проведение математического анализа эксплоитов ставит своей целью не только описание текущего состояния в данном секторе информационной безопасности, но и определение тренда, поскольку фундаментальных изменений в области информационной безопасности не ожидается вплоть до обновления принципов функционирования электронных вычислительных машин. Поэтому существующие тенденции, хорошо прослеживаемые по набранной на текущий день статистике для мобильных и компьютерных ОС, будут справедливы и при экстраполяции их на последующие версии ОС и сервисного программного обеспечения.

Динамика появления и закрытия уязвимостей в программном обеспечении определяется следующими характеристиками:

- все выявленные уязвимости к очередному мажорному обновлению (т.е. обновлению в первой или во второй цифре версии) ОС становятся закрытыми;
- появление новых уязвимостей практически целиком связано с появлением дополнительного функционала;
- выявление сквозных уязвимостей (т.е. уязвимостей, справедливых и для предыдущей, и для новой версии ОС) можно считать пренебрежимо малым;
- выявление уязвимостей методом patch-diffing, когда анализируется обновленный код и строятся предположения об уязвимостях, которые он закрывает относительно старых версий, позволяет нарушителю обнаруживать так называемые уязвимости первого дня, которые нашли и закрыли сами разработчики;
- выявляемость уязвимостей нулевого дня, как правило, для каждой конкретной разработки определяется архитектурой решения, и от версии к версии варьируется незначительно.

Исходя из вышеизложенного, можно составить математическую модель количества эксплуатируемых уязвимостей для заданной версии ОС или сервисного программного обеспечения. Количество эксплуатируемых уязвимостей рассматривается как мощность приведенного ниже множества.

$$E_V = K_0 \cup K_1, \quad (4)$$

где E_V – множество уязвимостей для данной версии «V» операционной системы ОС или программного обеспечения, K_0 – множество уязвимостей нулевого дня для данного программного обеспечения, K_1 – множество уязвимостей первого дня для данного программного обеспечения.

Важно отметить, что в любой момент времени подверженность конкретной версии ОС или сервисного программного обеспечения уязвимостям нулевого и первого дня может быть оценена также по имеющейся в сети информации о продаже соответствующих уязвимостей.

Зная количество эксплуатируемых уязвимостей, можно составить функцию атаки для злоумышленника, использующего эксплоиты, исходя из следующих критериев:

- каждый эксплоит имеет конечную скорость выполнения, зависящую от конкретного типа эксплоита;
- злоумышленник использует стандартный набор эксплоитов, часть из которых является неприменимой на данной платформе, что приводит, исходя из первого пункта, к потере времени в ходе выполнения атаки.

Принимая во внимание, что $f_Э(t,X)$ – функция, значение которой равно вероятности того, что эксплоит будет найден за время t, тогда функция атаки на элемент X, для которого возможна эксплуатация программного обеспечения, в таком случае приобретает следующий вид:

$$\begin{cases} f_Э(t,X) = 0 \text{ при } t \in \left[0, \sum_i T(\{M \setminus E_V\}_i) \cup \right. \\ \left. \cup\ T(\{M \cap E_V\}_0)\right] \\ f_Э(t,X) = 1 \text{ при } t \geq \sum_i T(\{M \setminus E_V\}_i) \cup \\ \cup\ T(\{M \cap E_V\}_0) \end{cases}, \quad (5)$$

где M – множество эксплоитов, которыми владеет злоумышленник,

T – отображение множества эксплоитов на множество соответствующих им времен выполнения T,

$\{M \setminus E_V\}_i$ – множество эксплоитов, которые есть у злоумышленников, но которые не применимы к рассматриваемой системе,

$\{M \cap E_V\}_0$ – множество эксплоитов, походящих к рассматриваемой системе.

Как видно из функции атаки, принципиальную возможность получения атакующим несанкционированного доступа методом применения эксплоитов можно оценить априорно, зная конкретную версию «V» ОС, используемой пользователем или установленной на сегменте инфраструктуры сотовой сети, а также множество M эксплоитов злоумышленника. Возможность получения мошенником несанкционированного доступа существует, когда пересечения множества эксплоитов правонарушителя и уязвимостей ОС не равно нулевому множеству.

Проведем обобщение функции атаки до случая, когда на атакуемой системе, помимо базового программного обеспечения, установлено также сервисное программное обеспечение, также имеющее уязвимости:

$$\begin{cases} f_Э(t,X) = 0 \text{ при } t \in \left[0, \sum_i T(\left\{M \setminus \cup_j E_{jV}\right\}_i) \cup \right. \\ \left. \cup\ T(\left\{M \cap \cup_j E_j(V)\right\}_0)\right] \\ f_Э(t,X) = 1 \text{ при } t \geq \sum_i T(\left\{M \setminus \cup_j E_{jV}\right\}_i) \cup \\ \cup\ T(\left\{M \cap \cup_j E_j(V)\right\}_0) \end{cases}, \quad (6)$$

где $E_{j\,V}$ – набор эксплоитов для j программного обеспечения, используемого на объекте атаки.

Здесь мы переходим от одного множества уязвимостей ОС к набору множеств, включающих уязвимости сервисного программного обеспечения.

Перечислим методы, которыми, исходя из математической модели, можно воспользоваться для снижения вероятности поражения системы путем атак посредством эксплоитов:

- использование последних версий программного обеспечения позволяет исключить из списка эксплоитов уязвимости, обнаруживаемые посредством patchdiffing (то есть уязвимости первого дня);
- снижение количества сервисного программного обеспечения также снижает вероятность успешной атаки эксплоитов;
- принципиально другой подход – использование различных моделей защиты данных непосредственно внутри системы, предполагающих наличие доступа злоумышленника к данным.

В последнем случае такой моделью защиты данных внутри системы является, например, модель Белла-ла-Падула, также известная как мандатная модель доступа к данным.

Атаки с использованием дополнительного оборудования

Получение несанкционированного доступа к данным посредством использования дополнительного оборудования, а именно – «виртуальных» сот, заставляющих мобильное устройство переключиться с базовой станции сотового оператора на поддельную базовую станцию, является специализированной атакой, которая может быть проведена исключительно на мобильные устройства.

В ходе атаки злоумышленник получает доступ ко всему трафику данных, в нормальном режиме протекающему через ССПС, – голосовые данные, данные пакетного обмена и короткие сообщения (включая USSD-сообщения, в нормальном режиме считающиеся защищенными и даже используемые банкоматами для передачи чувствительных данных).

Поскольку виртуальная сота не имеет средств активного воздействия на мобильное устройство, атака посредством нее относится к классу сниффинг-атак.

Представим функцию атаки с использованием виртуальной соты в следующем виде:

$$f(t,r), \tag{7}$$

где t – время, r – длина радиус-вектора с начальной точкой в центре круговой области A радиуса R, где располагается виртуальная сота, и конечной точкой в месте расположения мобильного устройства в данный момент времен $t \in [0, t']$.

При этом принимаются следующие допущения.

Движение мобильного устройства осуществляется со скоростью v с постоянным модулем $|\overline{v}|$ по непрерывной кусочно-линейной траектории внутри области A; v – проекция вектора скорости v на радиус-вектор r, $r \in [0, \infty]$. Начальная точка радиус-вектора совпадает с положением виртуальной соты, а конечная – с текущим положением мобильного устройства.

На мобильном устройстве на всем интервале времени $[0, t']$ имеется фиксированный объем информации V. Раскрытие ее при $v = 0$ происходит с постоянной скоростью $k_2 = \frac{\Delta V}{T}$. Степень раскрытия информации есть $f = \frac{\Delta V}{V} \le 1$. Поэтому степень раскрытия информации может быть описана функцией

$$f(t) = k_2 t \tag{8}$$

Полагая

$$r(t) = r(0) + vt \tag{9}$$

можно предложить при $v \neq 0$ следующий вид функции атаки

$$f(t,r) = k_1 \frac{k_2 t}{(r(0) + (v\ t))^{\alpha}} \tag{10}$$

где k_1 – положительный коэффициент, определяемый экспериментально, $0 < \alpha \le 1$. Показатель степени α. является функцией времени, например $\alpha = 1 - \exp(-(r(0) + vt))$

Поскольку раскрытие информации идет при любом значении *v*, то модифицируем формулу 10 так, чтобы ее можно было использовать как при $v = 0$, так и при $v \neq 0$.

Пусть $\{[t_{i_k},\ t_{i_k+1}]\}$ – множество всех отрезков времени, на которых $v \neq 0$, где *k = 1, ... N; i_1=1; i_k=i_{k-1}+2*. Тогда перепишем (10) в виде

$$f(t,r) = k_1 \frac{k_2 t}{(r(t_{i_k}) + v(t_{i_k} - t_{i_k+1}))^{\alpha}} \tag{11}$$

На основании данного представления можно сформулировать рекомендации по обеспечению безопасности мобильного устройства от угрозы получения злоумышленником несанкционированного доступа к данным посредством виртуальной соты:

- программное определение нахождения телефона в зоне действия виртуальной соты должно за минимальное время определить факт наличия прослушивающего оборудования;
- наибольшей опасности подвергается абонент, продолжительное время перемещающийся в небольших пределах. Для критических объектов обнаружение виртуальной соты должно выполняться стационарными средствами.

Модели атаки с использованием аппаратных и программных закладок

Математическая модель нарушителя, использующего аппаратные или программные закладки, достаточно просто реализуется с учетом предложенных в предыдущих пунктах подходов.

DOI:10.21681/2311-3456-2021-6-62-67

Очевидно, что наличие закладки позволяет злоумышленнику в теории иметь постоянный доступ к данным, хранимым или обрабатываемым в системе. Будем считать, что время начала передачи полученных в результате действий закладки данных пренебрежимо мало, так же, как и мало время передачи самих данных. Такое предположение можно считать верным, если учитывать специфику мобильных средств связи.

Но при этом очевидно, что любая закладка имеет так называемое время активации, то есть время, начиная с которого закладка начинает активный сбор данных и их передачу. Это время стоит выделить отдельно, так как именно момент активации закладки может быть идентифицирован и явиться поводом к ответным мерам со стороны защищающейся стороны. Обозначим такое время как T_a. Тогда возможно следующее утверждение

$$f_7(t, X) = \begin{cases} 1, t \geq T_a \\ 0, t < T_a, \end{cases} \quad (12)$$

где X – элемент сети СПСС, для которого может быть актуальна атака с использованием закладки.

Очевидно, что основными мерами по обеспечению защиты данных абонента ССПС должны заключаться в использовании верифицированного программного обеспечения, которое гарантированно не имеет закладок, либо сервисного ПО, способного в кратчайшие сроки обнаружить активацию или факт несанкционированной передачи данных.

Рассмотрев перечень базовых атак на мобильные устройства, можно сказать, что методы математического моделирования позволяют систематизировать подход к классификации атак. Использование приведенных подходов и моделей позволит таргетировано подбирать эффективные методы защиты от таких атак.

Заключение

Математическое обоснование и формализация моделей наиболее распространенных атак на мобильные устройства закладывает основу для разработки методов защиты от атак.

Анализ же существующих атак и методов защиты позволяет предложить целесообразность разработки и использования ряда технических решений для осуществления защиты информации, а именно:

- виртуального оператора защищенной связи, построенного на базе концепции виртуального оператора связи (MVNO, от англ. Mobile virtual network operator), который позволяет перейти на доверенное оборудование оператору связи и осуществить защиту каналов передачи данных;
- специального средства обнаружения виртуальных сот в радиоканале;
- доверенной ОС для мобильных устройств;

Кроме того, предлагается целесообразной модификация существующих технических решений защиты в части добавления в них:

- метода защиты аппаратной платформы для мобильных устройств с использованием специализированного аппаратного фильтра;
- новых технических решений по обеспечению антивирусной защиты.

Путем выполнения вышесказанного могут быть сформированы базовые принципы предотвращения и нейтрализации вторжений в систему мобильных устройств.

Рецензент: *Язов Юрий Константинович, доктор технических наук, профессор, ГНС ГНИИИ ПТЗИ ФСТЭК России, г. Воронеж, Россия. E-mail: yazoff_1946@mail.ru*

Литература

1. Баженов С.В., Коровин С.Д., Сухов А.В., Макеев В.И., Омск, 2012. Проблемы защиты современных средств связи / Омск, Академия военных наук, 2012. 104 с.
2. S. J. Alsunaidi and A. M. Almuhaideb, “Security Methods Against Potential Physical Attacks on Smartphones,” 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1-6. DOI: 10.1109/CAIS.2019.8769458
3. Егорова А.И., Борисенко П.С., Атаки по сторонним каналам на смартфоны на примере электромагнитных атак и методы противодействия им // Сборник трудов VII Конгресса молодых ученых. Санкт-Петербург. 2018. С. 45-47.
4. Бутакова Н.Г., Ситников Т.А. Анализ причин уязвимости мобильных приложений и средства защиты // REDS: Телекоммуникационные устройства и системы. 2016. Т. 6. № 4. С. 534-537.
5. Михайлов Д.М., Фесенко С.Д., Жуков И.Ю., Насенков И.Г. Воздействие внедренных программных закладок на безопасность мобильных телефонов // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 86-90.
6. Мостовой Р.А., Левина А.Б., Слепцова Д.М., Борисенко П.С. Атаки по сторонним каналам на мобильные телефоны // Вестник компьютерных и информационных технологий. 2019. № 12 (186). С. 46-53.
7. Бельтов А.Г., Жуков И.Ю., Михайлов Д.М., Стариковский А.В., Толстая А.М. Атаки на мобильные телефоны, использующие механизм автоматической настройки // Безопасность информационных технологий. 2012. Т. 19. № 2S. С. 22-25.
8. Рапетов А.М., Шишин О.И., Аристов М.С., Холявин В.Б., Савчук А.В., Жорин Ф.В. Методы получения доступа к данным, хранимым на мобильном устройстве и обрабатываемым им // Спецтехника и связь. 2014. № 1. С. 7-13.
9. R. Spreitzer, V. Moonsamy, T. Korak and S. Mangard, “Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices,” in IEEE Communications Surveys & Tutorials, vol. 20, No.1, pp. 465-488, Firstquarter 2018. DOI: 10.1109/COMST.2017.2779824
10. J. Jose, T. T. Tomy, V. Karunakaran, Anjali Krishna V, A. Varkey and Nisha C.A., “Securing passwords from dictionary attack with character-tree,” 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 2301-2307. DOI: 10.1109/WiSPNET.2016.7566553.

APPROACHES TO MATHEMATICAL SIMULATION OF CYBER ATTACKS ON MOBILE DEVICES

Mikhailov D.M.[9], Dvoryankin S.V.[10], Chumanskaya V.V.[11]

The relevance of the topic of protecting mobile devices from cyber attacks is due to a significant increase in the number and share of mobile gadgets among modern devices for accessing the Internet.

The purpose of the article is to mathematically substantiate and formalize the models of the most common attacks on mobile devices. On the basis of the constructed models, methods are proposed to prevent and neutralize intrusions into the system of smartphones and tablet computers.

***Method:** applied system analysis of the results of generalization and classification of typical types of attacks on mobile devices, elements of the theory of probability.*

***Results:** the features of mechanisms for the formation of vulnerabilities of mobile devices were determined. The important aspects of determining the effectiveness of modern technologies for protecting against cyber attacks on mobile devices are identified. A brief overview of the main approaches to mathematical modeling of the most common attacks is given. Additional requirements are formulated for an adequate choice of protection methods depending on the type of attacks. Recommendations are formulated to ensure the security of a mobile device against threats. Methods for reducing the probability of system damage by the most common attacks are proposed.*

***Keywords:** smartphone, tablet, digital economy, digital infrastructure, brute-force attacks, exploit programs, hardware and software bookmarks, methods of protection against attacks, organizational protection measures, technical protection measures, identification of vulnerabilities.*

References

1. Bazhenov S.V., Korovin S.D., Sukhov A.V., Makeev V.I. Poblemy zashchity sovremennykh sredstv svyazi / Omsk, Academy of Military Sciences, 2012. 104 p.
2. S. J. Alsunaidi and A. M. Almuhaideb, “Security Methods Against Potential Physical Attacks on Smartphones,” 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), 2019, pp. 1-6. DOI: 10.1109/CAIS.2019.8769458
3. Yegorova E.I., Borisenko P.S. Ataki po storonnim kanalam na smartfony na primere elektromagnitnykh atak I metody protivodeystviya im // In the collection: Collection of works of the VII Congress of young scientists. St. Petersburg, 2018. P. 45-47.
4. Butalova N.G., Sitnikov T.A. Analiz prichin uyazvimosti mobilnykh prilozheniy I sredstva zashchity // REDS: Telecommunication devices and systems.2016. T. 6. № 4. P. 534-537.
5. Mikhaylov D.M., Fesenko S.D., Zhukov I.Y., Nasenkov I.G. Vozdeystvie vnedrennykh programmnykh zakladok na bezopasnost mobilnykh telefonov // Information security problems. Computer systems. 2015. № 2. P. 86-90.
6. Mostovoy R.A., Levina A.B., Sleptsova D.M., Borisenko P.S. Ataki po storonnim kanalam na mobilnye telefony // Bulletin of Computer and Information Technologies. 2019. № 12 (186). P. 46-53.
7. Beltov A.G., Zhukov I.Y., Mikhaylov D.M., Starikovskiy A.V., Tolstaya A.M. Ataki na mobilnye telefony, ispolzueshchie mekhanizm avtomaticheskoy nastroyki // Information technology security. 2012. T. 19. № 2S. P. 22-25.
8. Rapetov A.M., Shishin O.I., Aristov M.S., Kholyavin V.B., Savchuk A.V., Zhorin F.V. Metody polucheniya dostupa k dannym, khranimym na mobilnom ustroystve i obrabatyvaemym im // Special equipment and communication. 2014. № 1. P. 7-13.
9. R. Spreitzer, V. Moonsamy, T. Korak and S. Mangard, “Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices,” in IEEE Communications Surveys & Tutorials, vol. 20, No.1, pp. 465-488, Firstquarter 2018. DOI: 10.1109/COMST.2017.2779824
10. J. Jose, T. T. Tomy, V. Karunakaran, Anjali Krishna V, A. Varkey and Nisha C.A., “Securing passwords from dictionary attack with character-tree,” 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 2301-2307. DOI: 10.1109/WiSPNET.2016.7566553

[9] Dmitry M. Mikhailov, Ph.D., Expert of the China Branch of BRICS Institute of Future Networks, Shenzhen, China. E-mail: mikhaylovdm@bifnc.cn

[10] Sergey V. Dvoryankin, Dr.Sc., Professor, Chief Researcher of the Institute of Information Sciences of the Moscow State Linguistic University, Moscow, Russia. E-mail: DvoryankinS@linguanet.ru

[11] Vera V. Chumanskaya, Postgraduate student of the Federal State Budgetary Scientific Institution “National Research Institute of World Economy and International Relations named after E.M. Primakov of the Russian Academy of Sciences”, Moscow, Russia. E-mail: vera.chumanskaya@gmail.com