Виктор А. Хвостов[1], Алексей В. Скрыпников[2], Евгений А. Рогозин[3],
Людмила А. Обухова[4], Дмитрий Г. Силка[5]
[1,2]ВГБОУ ВО «Воронежский государственный университет инженерных технологий»,
пр–т Революции, 19, Воронеж, 394036, Россия
[3,4,5]Воронежский институт МВД России,
пр–т Патриотов,53, Воронеж, 394065, Россия
[1]e-mail: hvahva1@mail.ru, https://orcid.org/0000-0002-9324-5415
[2]e-mail: skrypnikovvsafe@mail.ru, https://orcid.org/0000-0003-1073-9151
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535
[4]e-mail: obuhova.lyudmila@bk.ru, https://orcid.org/0000-0003-0198-4972
[5]e-mail: sdg.silka@gmail.com, https://orcid.org/0000-0001-5086-6433

АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ОБРАБОТКЕ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В МОБИЛЬНЫХ СИСТЕМАХ

DOI: http://dx.doi.org/10.26583/bit.2021.1.08

Аннотация. Проведен анализ мобильных технологий, используемых для повышения качества управления в банковской сфере, сервиса и государственном управлении. На основе анализа уязвимостей мобильных станций (смартфонов, планшетов, смарт устройств, различных периферийным устройств смартфонов и т.п.), технологий предоставления доступа к интернету для мобильных систем (используемые в сетях сотовой связи, беспроводного доступа), а также мобильных сервисов информационных систем предложена классификация угроз безопасности информации и проведен анализ возможностей по реализации этих угроз. Целью работы является разработка актуальной модели угроз безопасности мобильных технологий, проведение исследований по оценке полноты и непротиворечивости применяемых в настоящее время средств защиты мобильных систем, таких как менеджер мобильных устройств, менеджер мобильных приложений, магазин доверенных мобильных приложений, шлюз безопасности мобильных приложений и др. В статье рассматриваются источники угроз, уязвимости технологий мобильных систем, каналы воздействия угроз, объекты воздействия и возникающие ущербы от реализации угроз, характерные для мобильных систем и имеющие отличные от традиционной точки приложения реализаций угроз и векторы. Проведен анализ контекста применения мобильных технологий и влияния на процессы предоставления услуг.

Ключевые слова: мобильные системы, мобильная станция, шлюз безопасности, менеджер мобильных устройств.

Для цитирования: ХВОСТОВ, Виктор А. и др. АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ОБРАБОТКЕ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ В МОБИЛЬНЫХ СИСТЕМАХ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 95–105, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1324>. Дата доступа: 05 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.08.

Victor A. Khvostov[1], Alexey V. Skrypnikov[2], Evgeniy A. Rogozin[3],
Ludmila A. Obuhova[4], Dmitriy G. Silka[5]
[1,2]Voronezh State University of Engineering Technologies,
Revolution Avenue, 19, Voronezh, 394036, Russia
[3,4,5]Voronezh Institute of the Ministry of the Interior,
Prospekt Patriotov, 53, Voronezh, 394065, Russia
[1]e-mail: hvahva1@mail.ru, https://orcid.org/0000-0002-9324-5415
[2]e-mail: skrypnikovvsafe@mail.ru, https://orcid.org/0000-0003-1073-9151
[3]e-mail: evgenirogozin@yandex.ru, https://orcid.org/0000-0002-4455-7535
[4]e-mail: obuhova.lyudmila@bk.ru, https://orcid.org/0000-0003-0198-4972
[5]e-mail: sdg.silka@gmail.com, https://orcid.org/0000-0001-5086-6433

Analysis of information security threats when processing confidential data in mobile systems

DOI: http://dx.doi.org/10.26583/bit.2021.1.08

Abstract. The analysis of mobile technologies used to improve the quality of management in the banking sector, service and public administration is carried out. Based on the analysis of vulnerabilities of mobile stations (smartphones, tablets, smart devices, various peripheral devices of smart phones, etc.), technologies for providing Internet access for mobile systems (used in cellular networks, wireless access), as well as mobile services of information systems. A classification of information security threats is proposed and an analysis of the possibilities for implementing these threats is carried out. The aim of the work is to develop an up-to-date model of security threats to mobile technologies and to study the completeness and consistency of currently used mobile system protection tools, such as a mobile device manager, mobile application manager, trusted mobile application store, mobile application security gateway, etc. The paper discusses the sources of threats, vulnerabilities of technologies of mobile systems, the channels of exposure to threats, objects of exposure and the resulting damage from the implementation of threats that are characteristic of mobile systems and have different applications of threat implementations and vectors. The analysis of the context of the use of mobile medicine and the impact on the processes of providing medical services is carried out.

Keywords: mobile systems, mobile station, security gateway, mobile device manager.
For citation: KHVOSTOV, Victor A. et al. Analysis of information security threats when processing confidential data in mobile systems. IT Security (Russia), [S.l.], v. 28, n. 1, p. 95–105, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1324>. Date accessed: 05 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.08.

Введение

Анализ современного состояния мобильных систем показал, что все большую популярность приобретает движение, известное сегодня как BYOD (BringYourOwnDevice), означающее применение личных станций в профессиональной деятельности специалистами различных сфер деятельности. По результатам исследования [1], около 60% офисных работников пользуются мобильными устройствами не только для личных целей, но и для выполнения тех или иных рабочих задач.

При этом все многообразие мобильных технологий можно условно разделить на следующие направления [2–5]. Первая группа технологий используется для координации рабочих процессов, управления данными, доступа к корпоративным ресурсам. Технологии первой группы повышают эффективность работы пользователя, экономят его время, предоставляют оперативно справочную информацию, улучшают дистанционное взаимодействие внутри организаций и профессиональных групп. Вторая группа приложений используется для непосредственного взаимодействия с объектами физического мира (АСУ ТП – IndustrialControlSystems (ICS) или IndustrialAutomation and ControlSystems (IACS)). При этом организуется взаимодействие между элементами системы на разных уровнях представления. Третья группа технологий представляет собой информационно-справочные службы (в том числе экстренные). И четвертая группа представляет собой технологии для осуществления в терминальном режиме в качестве тонкого клиента с информационными системами (удаленное диагностирование, удаленное обслуживание и т.п.).

При организации функционирования мобильных технологий основной информацией, циркулирующей в технических средствах, является различная конфиденциальная информация (персональные данные, коммерческая тайна и др.), технологическая информация и ключевая информация криптографических протоколов различного вида.

Таким образом, использование мобильных технологий связано с организацией обработки конфиденциальной информации различного содержания и требует применения организации защиты информации[1,2,3].

Анализ нормативных и законодательных документов России в области защиты конфиденциальной информации и вопросов защиты информации (ЗИ), показал, что в настоящее время методических рекомендаций по ЗИ в информационных системах, использующих мобильные технологии, не существует. Применяемые в информационных системах средства ЗИ, обеспечивающие безопасность мобильных компонентов, применяются без законодательного и методического обоснования.

В соответствии со сложившимся методическим подходом обеспечения ЗИ[4,5], начальным этапом является разработка модели угроз безопасности информации (БИ), содержащей как классификацию угроз, так и краткое описание реализации наиболее актуальных угроз.

Таким образом, целью статьи является разработка модели угроз БИ для информационных систем, применяющим BYOD технологии.

Уязвимости мобильных технологий, новые векторы реализации угроз БИ, классификация угроз.

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к конфиденциальной информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Угроза БИ может быть представлена в виде формальной записи следующего вида: угроза НСД в ИСПДн: = <источник угрозы>, <уязвимость ИСПДн>, <способ реализации угрозы>, <объект воздействия (программа, протокол, данные и др.)>, <деструктивное действие>.

Источником угрозы может выступать пользователь, вредоносная программа, аппаратная закладка.

По отношению к мобильным технологиям пользователей можно разделить на ряд категорий.

Сотрудники учреждения. Данная категория пользователей получает доступ к данным и услугам организации с мобильного устройства. Уровень доступа для пользователей этой категории основывается на требованиях, обусловленных их должностными обязанностями, уровнем конфиденциальности информации, к которой сотрудник должен получить доступ, и необходимости доступа к этим данным с

[1]Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» //«Российская газета»№ 165 от 29.07.2006.

[2]Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды приказ директора ФСТЭК России от 14.03.2014 № 31.

[3]Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/ Общие положения» (принят и введен в действие распоряжением Банка России от 17.05.2014 № Р-399.

[4]ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

[5]Методический документ ФСТЭК России. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008.

использованием мобильного устройства. Для сотрудника учреждения необходим набор мобильных учетных данных, которые используются для доступа к внутренним ресурсам информационной системы.

Партнеры – это сотрудники сторонних организаций, которые сотрудничают с организацией при выполнении определенных задач, включая технический персонал, поддерживающий работоспособность технических средств. Пользователям-партнерам может потребоваться доступ к системе, приложениям и инфраструктуре для выполнения назначенных технического обслуживания и регламентных работ, но им не предоставляется доступ и права, как для сотрудников. Пользователям-партнерам обычно предоставляется ограниченный набор мобильных учетных данных, которые используются для доступа к внутренним системам организации.

Внешние пользователи – это лица, которые не связаны с организацией, но которым необходим доступ к общедоступным данным организации через предоставляемые и поддерживаемые организацией интерфейсы. Этими интерфейсами обычно являются WEB-приложения или другие приложения для мобильных устройств. Внешние пользователи обычно не указывают свои учетные данные в мобильной информационной системе. Интерфейсы данных организации могут иметь набор локально используемых учетных записей, которые действительны только для ресурса, к которому осуществляется доступ.

Поставщики компонентов, сборок и аксессуаров мобильных устройств. Данная категория источников угроз ИБ имеет возможность физически вмешиваться в работу мобильного устройства перед его поставкой и устанавливать вредоносное программное обеспечение.

Поставщики услуг сервисов беспроводных технологий. Эта категория источников угроз опасна возможностью установки вредоносного программного обеспечения, направленного как на воздействие на данные пользователей, так и на процессы управления мобильным устройством. Поставщик услуг сервисов беспроводных технологий имеет возможность перенастройки мобильного устройства, получения доступа к информационному ресурсу мобильной станции, кэширования данных пользователя на носителе. При этом могут использоваться не только каналы передачи информации, использующие IP транспорт (MMS/SMS), но и каналы управления мобильной сети.

Наиболее опасным источником угроз БИ для мобильных технологий является вредоносный код (эксплойты, руткиты и др.). Это программное обеспечение, созданное с целью выполнить несанкционированное действие, которое может поставить под угрозу конфиденциальность, целостность или доступность мобильного устройства. Вредоносное ПО может быть прикреплено к мгновенным сообщениям, добавлено в электронную почту или загружено в интернет как зараженный файл. Вредоносное ПО также может быть встроено в загруженные приложения. Эта категория источников угроз БИ может повлиять на работу операционной системы мобильного устройства, компрометировать данные или приложения на мобильном устройстве или и то, и другое.

1. Основные уязвимости БИ мобильных технологий.

В качестве основных уязвимостей БИ мобильных технологий необходимо рассмотреть следующие:

– уязвимости беспроводных технологий, обеспечивающих доступ в интернет мобильных устройств;

– уязвимости мобильных устройств;

– уязвимости сервисов мобильного доступа информационных систем.

Уязвимости беспроводных технологий – это уязвимости, которые могут использоваться источником угрозы через сеть на уровне приложений или в приложениях, файлах документов или данных (как протоколов передачи данных, так и протоколы управления), как, а также с использованием протоколов управления мобильных устройств. Сетевые угрозы безопасности связаны с уязвимостями внутри сети и сетевых протоколов, а также устройств, приложений и данных, которые находятся в сети. Использование мобильных устройств актуализируют проблему анализа угроз безопасности на основе сети, поскольку для передачи цифрового потока используются сотовая связь, технологии WiFi, Bluetooth, InfraredCommunication (IR), NearFieldCommunication (NFC), имеющие ряд специфических уязвимостей и имеющих достаточно низкий уровень защищенности.

Мобильные устройства передают цифровой поток через сотовые сети. Соответственно, им свойственны уязвимости глобальной системы мобильной связи GSM [6–8], обеспечиваемой провайдером, цифровой технологии беспроводной передачи данных для мобильной связи, функционирующей как надстройка над 2G и 2.5G EDGE, универсальной системы мобильной связи (UMTS), технологии высокоскоростного пакетного доступа HSDPA и ее варианта HSUPA. Также могут быть рассмотрены уязвимости технологий сотовой связи с множественным доступом с кодовым разделением CDMA, в которых используются протоколы Evolution-Data Optimized (EV-DO) и Long-Term Evolution (LTE).

Передача данных и голоса по управляемой сети мобильных операторов может быть перехвачена, а конфигурация, а также основные компоненты могут быть скомпрометированы через каналы управления.

Мобильные устройства используют беспроводную сетевую связь Wi-Fi, основанную на семействе стандартов IEEE 802.11a/b/g/n. Эти устройства могут подключаться к любой мобильной точке доступа, персональным или корпоративным точкам доступа или аналогичным устройствам для одноранговой связи. Устройства, использующие связь Wi-Fi, уязвимы для перехвата другими устройствами Wi-Fi и беспроводными программными средствами, а также анализаторами сигналов[6]. Нелегитимные точки доступа (несанкционированные мошенники в административно управляемом домене) также представляют потенциальную угрозу, подвергая мобильные устройства угрозам «человек посередине».

Bluetooth[7]. Беспроводная технология малого радиуса действия Bluetooth, обеспечивает стандартный протокол замены проводов для подключения. Технология используется как для передачи данных между устройствами в персональной сети, так и для команд, а также для голосовой связи между устройством и гарнитурой. Bluetooth обеспечивает собственные механизмы шифрования и аутентификации, но также имеет известные уязвимости и угрозы БИ, такие как атака с перехватом ключей во время инициализации сеанса.

Инфракрасный порт (InfraRed Data Association – IrDA)[8,9]. Технология IrDA предоставляет спецификации для реализации передачи данных на физическом и канальном уровнях с использованием в качестве среды передачи инфракрасный диапазон световых

[6]K. Scarfone, D. Dicoi Wireless Network Security for IEEE 802.11a/b/g and Bluetooth (Draft). Recommendations of the National Institute of Standards and Technology. Special Publication 800-48 Revision 1 (Draft)
[7]NIST SP 800 121 Guide to Bluetooth Security. Published Date: May 2017.
[8]IrDA Marketing Requirements – Basis for the IrDA Technical Standards, Version 3.2 The Infrared Data Association, November 23, 1993.
[9]LAN Access Extensions for Link Management Protocol (IrLAN), Proposal, Version 1.0 The Infrared Data Association, January 1, 1996.

волн, но также имеет известные уязвимости спецификаций IrLAP, IrLMP, IrCOMM, Tiny TP, IrOBEX, IrLAN, IrSimple и IrFM, которые необходимо учитывать.

Инфракрасное излучение используется как для передачи данных между устройствами внутри локальной сети (PAN), так и для команд (односторонняя передача). Инфракрасный порт не предоставляет механизмов шифрования и аутентификации и, следовательно, имеет известные уязвимости. Большинство угроз БИ, связанные с уязвимостями IrDA зависят от поставщика, например, из-за переполнения буфера в принимающем коде инфракрасной связи.

Near field communication, NFC[10] («коммуникация ближнего поля», «ближняя бесконтактная связь») – технология беспроводной передачи данных малого радиуса действия, которая даёт возможность обмена данными между устройствами на расстоянии порядка 10 см. Данная технология представляет собой набор стандартов для маломощного, миниатюрного подключения для замены проводов для двухточечной связи, мобильных устройств.

Уязвимости NFC связаны с тем, что стек протоколов технологии не предусматривает использования криптографических протоколов при передаче. Стандарты хранения данных в метках и картах, а также их эмуляции – не предусматривают криптографической защиты при хранении.

В NFC сервисах традиционно закладывается излишнее доверие к информации, хранящейся в мобильном устройстве, в результате фактически не выполняется фильтрация данных. Подключение NFC в первую очередь подвержено атакам физического уровня, таким как перехват и внедрение сигналов, но конкретные реализации могут содержать дополнительные уязвимости.

Уязвимости мобильных систем. Уязвимости мобильных систем можно классифицировать по признаку принадлежности к элементу мобильной системы. При этом можно выделить уязвимости аппаратной составляющей мобильной станции, уязвимость мобильной операционной системы, уязвимость мобильного приложения.

Уязвимости аппаратной составляющей мобильной станции в основном связаны с ошибками или с преднамеренно установленными аппаратными люками при прошивке мобильной станции. Кроме того, в мобильных станциях могут быть установлены дополнительные несанкционированные аппаратные закладки, различные функции слежения и перехвата информации.

Уязвимость мобильной операционной системы и мобильных приложений аналогичны тем, что существуют для традиционных ЭВМ и постоянно обнаруживаются [9, 10]. Уязвимости операционной системы могут быть использованы аналогично уязвимым приложениям. Уязвимости операционной системы представляют большую угрозу, поскольку операционная система работает с более высоким уровнем привилегий, чем приложения. Мобильные приложения, как и приложения на других устройствах, также могут быть плохо написаны и уязвимы для атак и эксплуатации. Многие приложения уязвимы из-за ошибок программирования, ошибок проектирования или выбора конфигурации в возможностях обеспечения безопасности.

Кроме того, пользователи отключают встроенные функции безопасности ОС, обычно известные как «джейлбрейк» или «рутинг». Отключение встроенных функций безопасности ОС позволяет пользователям устанавливать приложения и усовершенствования системы, которые в противном случае были бы ограничено.

[10]ISO/IEC 18092 / ECMA-340 Near Field Communication Interface and Protocol-1 (NFCIP-1).

Существует высокий уровень риска, связанный с использованием измененных устройств с отключенными функциями безопасности мобильной ОС.

2. Основные каналы воздействия угроз БИ мобильных технологий

К основным каналам воздействия угроз БИ мобильных технологий относятся:

– физический доступ к мобильной станции;

– доступ к радиоканалу передачи цифрового потока от мобильной станции к базовой станции;

– доступ к высокоскоростным магистральным каналам передачи цифрового потока, используемым операторами сотовой связи;

– доступ к внутренней инфраструктуре информационной системы организации.

Основная уязвимость физического доступа к мобильной станции связана с доступом злоумышленника к данным при потере смартфона. Потеря мобильного устройства ставит под угрозу конфиденциальность, целостность и доступность информации. Кроме того, устройство может содержать учетные данные для доступа к информационной системе организации, что создает дополнительный риск для нее. Также, данные на мобильном устройстве могут быть потеряны, если устройство не выполняется резервное копирование.

Дополнительно, при возможности доступа злоумышленника к мобильной станции, возможна установка вредоносного аппаратного или программного обеспечения, которое может собирать или повреждать данные, как на устройстве, так и в информационной системе организации. Злоумышленник может использовать внешние интерфейсы для подключения мобильного устройства к USB и Bluetooth-модему. Кроме того, злоумышленник может подключить компьютер или внешний жесткий диск для клонирования, копирования, уничтожения, удаления или изменения содержимого мобильного устройства.

Существующие уязвимости встроенных функций мобильного устройства, таких как камера и микрофон, создают повышенную угрозу безопасности, создавая средства для сбора конфиденциальных изображений или разговоров. Также угрозу безопасности повышают уязвимости периферийных устройств, физически взаимодействующих с мобильной станцией (док-станции, гарнитуры, дополнительное оборудование).

Канал реализации угрозы БИ при доступе к радиоканалу передачи цифрового потока от мобильной станции к базовой станции представляет собой электронное прослушивание через беспроводную сеть (Wi-Fi или GSM), цифровой поток или речевые сигналы могут изменяться, ими можно манипулировать или выборочно блокировать во время передачи.

Канал побочных электромагнитных излучений. Мобильные станции основаны на работе различных дискретных электрических компонентов внутри самого устройства. Также они излучают внеполосные и кратные сигналы, соответствующие их основным радиоинтерфейсам, таким как сотовая связь, Bluetooth, NFC или Wi-Fi. Это излучение находится в пределах радиочастотного спектра и может быть захвачено и декодировано, поскольку информация, излучаемая ЦП и его подсистемами, в основном не зашифрована. И, следовательно, канал побочных электромагнитных излучений является уязвимым для наблюдения третьей стороной как в непосредственной близости, так и на расстоянии (например, 100 м).

Кроме перехвата сигналов мобильных станций дополнительной угрозой БИ являются подавление приемников мобильных станций (любой беспроводной протокол, используемый на мобильном устройстве, подвержен помехам, включая GPS, сотовую связь, Wi-Fi и Bluetooth). Кроме того, специфической угрозой, воздействующей по радиоканалу,

является угроза наводнения (flood) при реализации которой в систему направляется большее количество информации, чем она может обработать.

Большинство мобильных устройств обеспечивают возможность определения реального географического местоположения электронного устройства (геолокации) в своих приложениях. Такие приложения могут быть использованы для отображения текущей позиции на карте, поиска близлежащих ресурсов или отслеживания пути пользователя. Еще более популярным среди пользователей является возможность приложений указывать маршруты движения. Эти службы определения местоположения могут разгласить местоположение устройства (или предоставить неточную информацию о местоположении пользователя устройства из-за внешних помех или манипуляций).

Канал реализации угрозы БИ со стороны сети провайдера сотовой связи приводит к возможности нарушения конфиденциальности и целостности информации, т.к. для работы используются высокоскоростные магистральные сети, являющиеся составной частью сетей связи общего пользования страны [11].

3. Объекты воздействия угроз БИ мобильных технологий

Объектами воздействия угроз БИ являются информационные ресурсы, содержащие персональные данные, конфиденциальную служебную информацию организации, а также технологическая информация, программно-технические средства обработки информации, средства защиты персональных данных (ПДн), каналы информационного обмена и телекоммуникации информационной системы. В зависимости от места нахождения объектов воздействия угроз их можно классифицировать на следующие виды:

– информационный ресурс, содержащийся в мобильной станции;

– цифровой поток, передаваемый по радиоканалу «мобильная станция – базовая – станция провайдера сотовой связи»;

– цифровой поток, передаваемый по радиоканалу «мобильная станция – точка – доступа Wi-Fi»;

– цифровой поток, передаваемый по сети провайдера сотовой связи;

– цифровой поток, передаваемый по высокоскоростным магистральным сетям, являющийся составной частью сетей связи общего пользования страны;

– цифровой поток, обрабатываемый в сети организации.

В зависимости от вида объекты воздействия угроз можно разделить на:

– открытые данные;

– данные, зашифрованные симметричным шифром (DES, AES);

– данные, зашифрованные ассиметричным шифром (A5) [6–8].

4. Классификация угроз БИ мобильных технологий

По виду деструктивных действий, воздействующих на конфиденциальную информацию в мобильных технологиях, традиционно выделяют следующие классы угроз БИ:

– приводящие к нарушению конфиденциальности;

– приводящие к нарушению целостности;

– приводящие к нарушению доступности.

При этом, необходимо рассмотреть ряд специфических угроз БИ, обусловленных применением мобильных станций и непосредственно не нарушающих состояние безопасности ПДн.

Состав элементов описания угроз БИ мобильных технологий представлен на рис. 1.

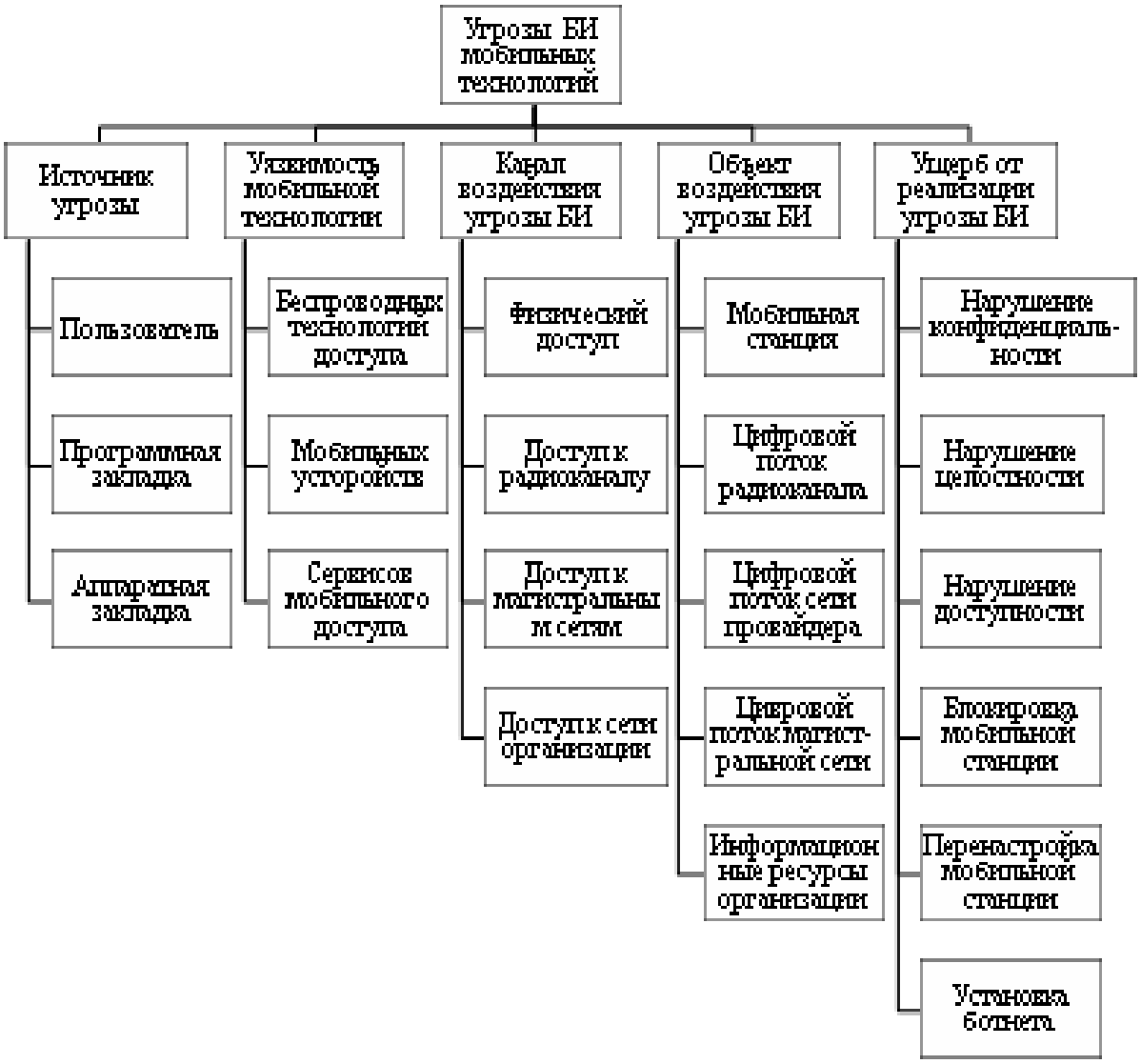

Рис. 1. Классификация угроз БИ мобильных технологий
Fig. 1. Classification of information security threats in mobile technologies

Мобильная станция в ходе функционирования передаёт в базовую станцию сервисную информацию (LAC, CellID, IMSI, NetworkIdentity and TimeZone и т.п.). Переданные мобильной станцией сервисные данные могут быть использованы для анализа поведения пользователя или организации (например, локальные и удаленные журналы). Также широко применяется специальное программное обеспечение и сервисы провайдеров мобильной связи для объединения данных геолокации с информацией SSID для сбора информации о местоположении определенных беспроводных сетей, которые совместно используются их клиентами. Известны примеры программного обеспечения, установленного поставщиком услуг сотовой связи, использующиеся для отслеживания поведения пользователя, а также показателей производительности мобильной станции или мобильного сервиса. Эти данные также могут быть отправлены непосредственно поставщику или третьей стороне.

В ходе использования мобильной станции пользователь может установить приложение, содержащее вредоносный код, позволяющий перенастроить мобильное

устройство (прямо или косвенно) или предлагать услугу непосредственно или через стороннее устройство.

Вредоносные программы, требующие выкуп, стали крайне распространенным классом злонамеренных программ для мобильных систем. Как правило, блокируется работа мобильной станции, требуя с жертвы выкуп, после выплаты которого возвращают пользователю контроль над смартфоном или планшетом. Также преступники выбирают в качестве целей истории звонков, контакты, фотографии или сообщения, что практически всегда вынуждает пользователя заплатить затребованную сумму.

Ботнеты, состоящие из взломанных мобильных станций – еще одна актуальная угроза БИ. Зараженные устройства, являющиеся частью ботнетов, находятся под контролем злоумышленников, которые в любой момент могут приказать им инициировать DDoS-атаку на какой-либо ресурс, либо начать массовую рассылку спам писем.

Заключение

Проведенный в статье анализ угроз БИ аппаратных и программных средств мобильных технологий, используемых в сфере сервиса, АСУ ТП и банковской сфере, показал значительное усложнение проблемы обеспечения БИ при существенном повышении эффективности функционирования при использовании этой технологии. Применение мобильных станций в качестве основного инструмента в сфере сервиса, АСУ ТП и банковской сфере, участие третьей стороны в процессах обработки конфиденциальной информации (провайдер услуг сотовой связи, провайдер услуг беспроводного доступа, организации, эксплуатирующие высокоскоростные магистральные каналы передачи цифрового потока) привело к существенному усложнению традиционной модели угроз БИ сформированной ФСТЭК России. Новые угрозы БИ, обусловленные использованием мобильных технологий и новые векторы реализации угроз, рассмотренные в статье, позволили доработать модель угроз БИ и разработать классификационную схему угроз БИ, представленную на рис. 1.

СПИСОК ЛИТЕРАТУРЫ:

1. Исследование мобильного интернета в России. URL: https://www.shopolog.ru/news/mail-ru-group-issledovanie-mobilnogo-interneta-v-rossii/ (дата обращения: 10.11.2020).
2. Никитин П.В., Мурадянц А.А., Шостак Н.А. Мобильное здравоохранение: возможности, проблемы, перспективы // Клиницист. 2015, № 4. С. 13–21. URL: https://www.elibrary.ru/item.asp?id=25672591 (дата обращения: 10.11.2020).
3. Яненко М.Б., Яненко М.Е. Мобильные технологии в маркетинге услуг: новые возможности и проблемы // Проблемы современной экономики. 2014. № 2. С. 227–230. URL: https://www.elibrary.ru/item.asp?id=21981140 (дата обращения: 10.11.2020).
4. Банковское обслуживание будущего: мобильные технологии стимулируют развитие инноваций. URL: https://www.intel.ru/content/www/ru/ru/financial-services-it/article/banking-on-the-future.html (дата обращения: 10.11.2020).
5. АСУ ТП с использованием мобильного телефона. URL: http://www.adastra.ru/products/overview/mobile/ (дата обращения: 10.11.2020).
6. Попов В.И. Основы сотовой связи стандарта GSM М.: Эко-Трендз, 2005. – 296 с.
7. Интеллектуальные сети связи. / Лихтциндер Б.Я. [и др.] М.: ЭКО-ТРЕНДЗ, 2000. – 205 с.
8. Шиллер Й. Мобильные коммуникации. М.: Вильямс, 2002. – 384 с.
9. Zhu X., Zhu Y. (2019) Extension of ISO/IEC27001 to Mobile Devices Security Management. In: Yun X. et al. (eds) Cyber Security. CNCERT 2018. Communications in Computer and Information Science. Vol. 970. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-13-6621-5_3.
10. Gkioulos, Vasileios; Wangen, Gaute; Katsikas, Sokratis K.; Kavallieratos, George; Kotzanikolaou, Panayiotis. 2017. "Security Awareness of the Digital Natives" Information 8, no. 2: 42. DOI: https://doi.org/10.3390/info8020042.

11. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи. Учебник для ВУЗов. СПб.: БХВ-Петербург. 2011. – 400 с.

REFERENCES:

[1] Research of the mobile Internet in Russia. URL: https://www.shopolog.ru/news/mail-ru-group-issledovanie-mobilnogo-interneta-v-rossii/ (accessed: 10.11.2020) (in Russian).
[2] Nikitin P.V., Muradyants A.A., Shostak N.A. Mobile health care: opportunities, problems, prospects. Clinician. 2015, no. 4. P. 13–21. URL: https://www.elibrary.ru/item.asp?id=25672591 (accessed: 10.11.2020) (in Russian).
[3] Yanenko M.B., Yanenko M.E. Mobile technologies in marketing services: new opportunities and problems. Problems of modern economics. 2014, no. 2. P. 227–230. URL: https://www.elibrary.ru/item.asp?id=21981140 (accessed: 10.11.2020) (in Russian).
[4] Banking services of the future: mobile technologies stimulate the development of innovations. URL: https://www.intel.ru/content/www/ru/ru/financial-services-it/article/banking-on-the-future.html (accessed: 10.11.2020) (in Russian).
[5] ACS TP using a mobile phone. URL: http://www.adastra.ru/products/overview/mobile/ (accessed: 10.11.2020) (in Russian).
[6] Popov V.I. Fundamentals of cellular communication of the GSM standard M.: Eco-Trends, 2005. – 296 p. (in Russian).
[7] Intelligent communication networks. Likhtzinder B.Ya. [and others] M.: EKO-TRENDZ, 2000. – 205 p. (in Russian).
[8] Schiller J. Mobile communications. M.: Williams, 2002. – 384 p. (in Russian).
[9] Zhu X., Zhu Y. (2019) Extension of ISO/IEC27001 to Mobile Devices Security Management. In: Yun X. et al. (eds) Cyber Security. CNCERT 2018. Communications in Computer and Information Science. Vol 970. Springer, Singapore. DOI: https://doi.org/10.1007/978-981-13-6621-5_3.
[10] Gkioulos, Vasileios; Wangen, Gaute; Katsikas, Sokratis K.; Kavallieratos, George; Kotzanikolaou, Panayiotis. 2017. "Security Awareness of the Digital Natives" Information 8, no. 2: 42. DOI: https://doi.org/10.3390/info8020042.
[11] Goldstein B.S., Sokolov N.A., Yanovskiy G.G. Communication networks. Textbook for universities. SPb.: BHV-Petersburg. 2011. – 400 p. (in Russian).

Поступила в редакцию –26 ноября 2020 г. Окончательный вариант – 05 февраля 2021 г.
Received –November 26, 2020. The final version – February 05, 2021.