УДК 004.056.5

МЕТОДИКА ОРГАНИЗАЦИИ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ НА МОБИЛЬНЫХ УСТРОЙСТВАХ

К.В. БРАУН, В.А. ЧАСТИКОВА

Кубанский государственный технологический университет,
350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
электронная почта: chastikova_va@mail.ru

В статье рассмотрены перспективы развития корпоративной мобильности и проблемы безопасности информации, связанные с этим направлением. Так как направление активно развивается в России, проблема защиты корпоративной информации является более чем актуальной. На основе того что обработка, хранение и передача информации на портативных устройствах имеет отличительные особенности, в работе проанализирован ряд методов в разных областях информационной безопасности - от оценки рисков до планирования организационных мер. Предложены и собраны в виде развернутой методики адаптированные алгоритмы расчета коэффициентов оценки безопасности на основе существующих математических методов исследования.
Ключевые слова: информационная безопасность, мобильные устройства, корпоративная мобильность, оценка рисков, модель угроз, удаленный доступ.

Все чаще компании внедряют в свои корпоративные сети для работы с информацией мобильные устройства. По данным исследования Gartner, проведенного в конце октября 2012 года, уже в 2017 году более двух третей предприятий во всем мире перейдут на мобильные устройства в работе с корпоративными системами управления.

Аналитики уверены, что более 65% предприятий будут использовать разнообразные решения для мобильных устройств, в частности для планшетов и смартфонов, в работе с корпоративными системами. Gartner прогнозирует, что к 2017 году 90% предприятий будут поддерживать две и более мобильные операционные системы для работы своих сотрудников.

Одной из основных причин роста этого направления стало бурное развитие рынка планшетных компьютеров. Если раньше пользователи планшетов ограничивались установкой корпоративной почты, то теперь все больше людей хотят внедрить на свои девайсы мобильные приложения корпоративных систем для работы в любом месте [1].

На рисунке 1 представлены наиболее востребованные функции с использованием мобильных устройств.

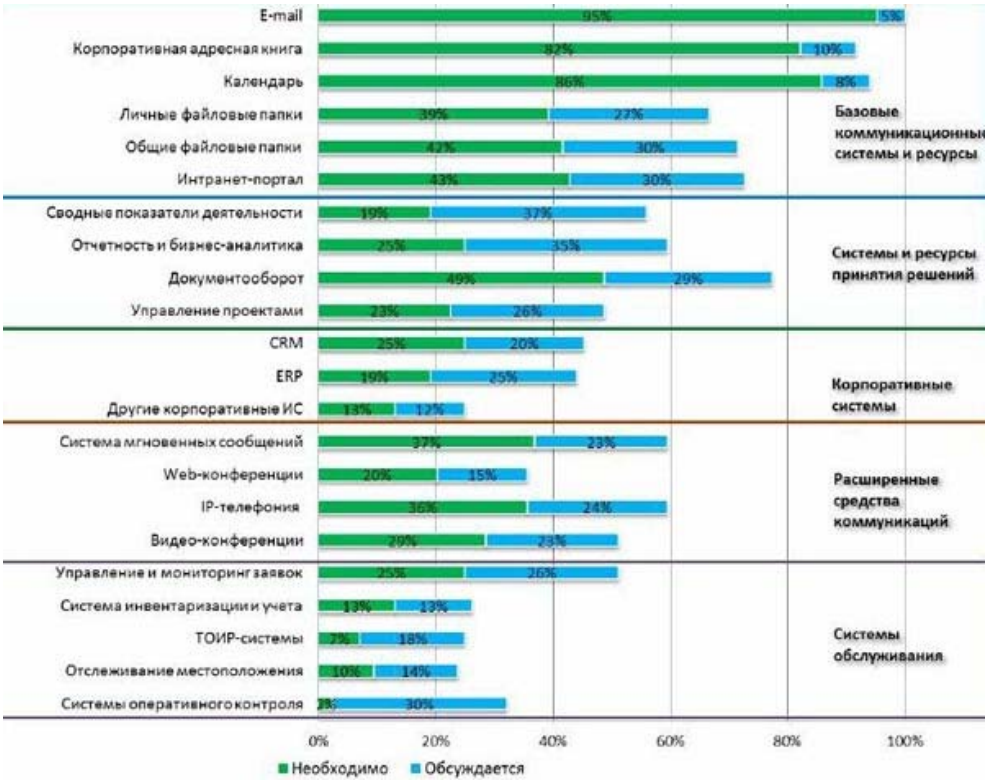

Рисунок 1 – Наиболее востребованные функции с использованием мобильных устройств

Необходимость защищать информацию на мобильных устройствах, особенно при их корпоративном применении, осознают не только специалисты по информационной безопасности, но и люди, не имеющие прямого отношения к этой отрасли. В то же время риски, связанные с внедрением публичных сервисов, очевидны сегодня далеко не всем, хотя они не менее высоки [2].

В России острую необходимость в использовании мобильных гаджетов в работе испытывают не все организации, а доверяют этому направлению с точки зрения безопасности еще меньше. Поэтому требуется взвешивать все за и против таких нововведений. Использование информации, таким образом, должно быть хорошо мотивировано, так как имеет свои риски безопасности и требует значительных затрат на организацию защиты.

В данной работе предлагаются алгоритмы оценки, анализа и выбора в виде методики, на основе представленной методики разработан программный комплекс.

На первом этапе предложенной методики собираются исходные данные, где заказчик формирует требования к типам устройств, предпочитаемой

концепции (BYOD, CYOD, COPE) и функционалу, желательно чтобы он проанализировал экономическую эффективность, рассчитал окупаемость и прибыль от введения данного сектора корпоративной мобильности и выразил это в процентах, где условно 0% - «нововведение ничего не изменит в бизнесе», а 100% - «очень необходимое нововведение, приведет к процветанию компании». Этот показатель назовем эффективностью использования (коэффициентом эффективности использования).

Специалист в области информационной безопасности должен проанализировать полученные данные и произвести собственную оценку. Основным критерием оценки будет являться безопасность применения. Она основывается прежде всего на типе обрабатываемой на устройстве информации: персональные данные (ПДн), коммерческая, служебная или иная тайна. Для них определена некоторая совокупность требований защиты, например для ПДн требования определяются исходя из уровня защищенности согласно Приказу ФСТЭК №21. В случае с другими видами тайн, требования к их защите могут быть сформированы в нормативных документах организации, либо отождествлены с ПДн.

Одним из вариантов расчета критерия безопасности может послужить расчет отношения требований безопасности, которые могут быть реализованы на устройстве локально к требованиям необходимым для данной категории информации согласно нормативным документам.

$$K_{Б} = \frac{\sum t_{P}}{\sum t_{K}}, \qquad (1)$$

где $K_Б$ – оценка безопасности;

t_K – меры, характерные для каждой категории информации;

t_P – меры, реализованные средствами операционной системой на устройствах;

В общую оценку по желанию можно включить дополнительные критерии, особенно когда в расчет не берется коэффициент эффективности

использования. Такими критериями могут быть удобство и функциональность. Функциональность определяет возможность выполнения бизнес-задач, удобство – повышение производительности и скорости реагирования. Расстановка значений данных критериев проводится экспертным методом специалиста безопасности. Каждый критерий рассчитывается по формуле:

$$G_i = \frac{\sum K_j \cdot q_j}{Q}, \quad (2)$$

где G_i – параметр составляющей оценки;

K_j – коэффициент составляющей для данного устройства;

q_j – количество устройств данного типа;

Q – общее число устройств.

Общая эффективность рассчитывается по формуле Гурвица:

$$Y = \mu \cdot \min(g) + (1 - \mu) \cdot \max(g), \quad (3)$$

где μ - коэффициент Гурвица, $0 < \mu < 1$;

g - величина параметров составляющих;

Причем величину μ определяет исследователь или лицо, принимающее решение. Затем данный показатель умножается на эффективность использования. Допустимым значением является 0,5 и выше. Общий результат позволит оценить целесообразность в отношении выгода/потеря и по возможности изменить исходные данные. При использовании разных типов устройств подход к обеспечению безопасности должен быть комплексным.

На основе типа устройств, требуемого функционала и обрабатываемой информации формируется модель угроз и производится оценка риска. При оценке рисков используют тот или иной математический аппарат: теорию вероятностей, теорию нечеткостей, интервальную математику [3].

Наиболее распространенным является подход на основе теории вероятностей, он в дальнейшем и будет применяться. В данном подходе используют вероятностную модель явления, описываемую случайным ущербом, коэффициентом безопасности и вероятностью события. В

вероятностной модели оценка возможности наступления нежелательного события (Р) сводится к вычислению вероятности и является безразмерной величиной от 0 до 1. Случайный ущерб описывается функцией распределения с бесконечно большим числом параметров (причин).

Случайный ущерб описывается функцией распределения с бесконечно большим числом параметров (причин). Параметрами функции могут быть характерные уязвимости с их вероятностью реализации или критичностью. Параметры взаимодействуют друг с другом аддитивно, т.е. вызванные ими эффекты складываются, тогда вероятности (веса) параметров согласно Центральной предельной теореме теории вероятностей подчиняются нормальному Гауссовому распределению.

Число параметров обычно пытаются сводить к небольшому числу, лучше всего к одному. С этой целью применяется вычисление математического ожидания (М).

Одним из вариантов оценки может стать составление матрицы покрытий угроз и выполняемого на мобильных устройствах функционала. Одному виду функции может быть присуще несколько типов угроз, так как реализация функций может затрагивать несколько технологий.

Пусть определено множество необходимых функций мобильного устройства $T=\{t_1,t_2,...,t_m\}$ и множество угроз, соответствующих данному типу устройств $Y=\{y_1,y_2,...,y_n\}$, таких, что каждый t_j ассоциирован с подмножеством $Y_j \subseteq Y$, где $j \in N=\{1,...,n\}$. Определим матрицу $A=(a_{ij})$:

$$a_{ij}=\begin{cases} M \cdot P \cdot (1-K_Б) \cdot \dfrac{n_i}{N}, если\ y_j\ соответствует\ t_i \\ 0, иначе \end{cases} \quad (4)$$

где М - математическое ожидание;

$К_Б$ – коэффициент безопасности;

n_i – число устройств приходящихся на функцию;

N – общее число устройств;

Р – возможность наступления нежелательного события.

Коэффициент n_i/N используется для нормирования значения риска по числу устройств. Так строится матрица покрытий, отраженная в таблице 1.

Таблица 1 – Матрица покрытий функций и угроз

	Угроза 1	Угроза 2	Угроза 3	Угроза 4	Угроза 5	Угроза 6	…	Угроза J	Число устройств приходящихся на данную функцию
Функция 1	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	…	$a_i/0$	n_1
Функция 2	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	…	$a_i/0$	n_2
Функция 3	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	…	$a_i/0$	n_3
Функция 4	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	…	$a_i/0$	n_4
Функция 5	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	…	$a_i/0$	n_5
….	…	…	…	…	…	…	…	…	…
Функция I	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	$a_i/0$	…	$a_i/0$	n_i
	k_1	k_2	k_3	k_4	k_5	k_6		k_j	

В последней строке рассчитывается средний показатель по столбцу. Этот показатель оценивает дальнейшее отношение к угрозе, насколько она актуальна и сколько устройств ей подвержены – k_j коэффициент значимости. Чем он выше, тем больше внимания нужно сосредоточить на этом и тщательнее выбирать средство/требование/функцию защиты; при минимальном показателе можно применять какие-либо универсальные средства, основной задачей которых является предотвращение другой угрозы.

Целью этой операции является распределение средств на защиту при ограниченности ресурсов, как финансовых, так и ресурсов производительности, и акцентирование внимания на критичном элементе. При использовании данной методики можно достаточно быстро определить, от какой функции стоит отказаться вследствие нецелесообразности ее использования.

Основные риски связаны с тем, что корпоративные данные хранятся и обрабатываются на устройствах, изначально не приспособленных для защиты со стороны корпоративных ИТ-служб. В случае утери или кражи устройства данные могут стать доступными злоумышленникам, а утерянный смартфон или планшет может открыть доступ к корпоративным приложениям или позволить подключиться к внутренней сети предприятия. Поэтому очень важно вовремя узнать о пропаже устройства, заблокировать его, очистить данные и проверить, не были ли скомпрометированы учетные записи халатного сотрудника [4].

Функции защиты можно условно разделить на базовые, обязательные и второстепенные. Базовые - это те функции, которые должны присутствовать в любом случае, чаще всего они необходимы для должного взаимодействия системы и устройства. Такие функции нужны независимо от набора угроз, выявленных ранее. К обязательным относятся функции, которые покрывают весь список угроз и выявленных уязвимостей, а также те функции, которые необходимо учесть согласно Приказу ФСТЭК при обработке ПДн.

Второстепенные функции - это функции, не являющиеся обязательными, однако они могут использоваться по нескольким причинам: повышение производительности, оптимизация и удобство управления, использование данной функции в дальнейшем, тестирование возможностей.

Функции защиты реализуются различными системами и технологиями. В общем виде можно представить безопасность мобильных устройств на основе формулы:

$$MS = EMM + К + App + OS + VPN + PS, \quad (5)$$

где MS – безопасность мобильных устройств;

EMM – Enterprise Mobile Management: MDM, MAM, MIM;

К – концепция использования МУ;

App – набор клиентских приложений;

OS – методы и средства защиты ОС;

VPN – средства защиты сети

PS – средства защиты ИС, связанные с обработкой информации на мобильных устройствах (DLP-системы, разграничение доступа и т.д.).

Для защиты данных на устройствах, таких как планшетный компьютер, смартфон, мобильный телефон, могут применяться одни решения EMM только в случае перекрытия всех угроз, но обычно они дополняются специализированным программным обеспечением, таким, как средства антивирусной защиты. Некоторые из них могут предложить и систему защиты для ноутбуков, но на практике оказывается, что это достаточно ограниченная система, реализующая только часть требований. Самыми яркими представителями на рынке являются AirWatch, MobileIron, IBM, Citrix. Российские разработчики также включились в процесс реализации подобных решений. Наиболее известные готовые продукты: Kaspersky Security for Mobile от «Лаборатории Касперского» и WorksPad Protected - совместное решение для создания защищенных корпоративных мобильных рабочих мест, созданное альянсом ИнфоТеКС, «МобилитиЛаб» (ГК АйТи) и НИИ СОКБ [5].

В отношении ноутбуков и нетбуков подход к защите реализуется подобно защите ПК с отличительной особенностью удаленного доступа и в случае концепции BYOD хранения личных данных на устройстве. То есть здесь рассматривается каждая конкретная подсистема защиты, и выбирается наиболее подходящее решение.

Выбор конкретного решения завит от финансовых ограничений предприятия и предпочтений по функционалу у специалиста, а также может быть реализован выбор подходящей системы с помощью существующих методик подбора компонентов.

После выбора системы защиты формируются рекомендации по эксплуатации и организационные меры. При информировании и обучении сотрудников стоит особое внимание уделить ответственности за нарушение требований. Помимо ценности информации, определяющим условием будет концепция применения МУ принятая на предприятии. Для концепции BYOD –

выдвигаются самые высокие требования, для CYOD – минимальные. Условно степень ответственности (X) можно представить в виде:

X_j = [Концепция МУ; ценность информации]

Для возможности совершенствования системы на основе исходных требований и возможных реализаций строится «идеальная» модель системы, в которой произведен поиск оптимального набора данных для повышения значения критерия эффективности (на первом этапе) и выбора наиболее подходящего технического решения без учета финансовых ограничений. На основе этой модели в дальнейшем могут производиться изменения системы защиты или вноситься изменения в систему до внедрения.

В целом, в статье описано большинство алгоритмов, которые уже используются в области ИТ и ИБ, основной же задачей методики является подборка наиболее подходящих методов оценки, анализа и обеспечения безопасности, а также адаптация этих методов для защиты информации на мобильных устройствах.

ЛИТЕРАТУРА

1 Mobile Device Management (MDM). Enterprise Mobility Management (EMM). Управление мобильными устройствами // TAdviser. ИТ-издание URL: http://www.tadviser.ru/index.php/Статья:Mobile_Device_Management_(MDM)_Управление_мобильными _устройствами_Enterprise_Mobility_Management_(EMM) (дата обращения 27.04.16).

2 Коржов В. Обзор продуктов компании ИнфоТеКС для защиты мобильных устройств // www.anti-malware.ru URL: https://www.anti-malware.ru/reviews/ViPNet_Client_for_Android_and_ViPNet_Connect (дата обращения 27.04.16).

3 Пугач О.В. Математические методы оценки рисков // Заводская лаборатория. Диагностика материалов. 2013, № 79. С. 64-69.

4 Чубуков А. Консьюмеризация в корпоративном секторе: насколько она безопасна? // www.pcweek.ru URL: http://www.pcweek.ru/security/article/ detail.php? ID=138037 (дата обращения 11.05.16).

5 Ференец В. Обзор рынка управления корпоративной мобильностью (EMM) в России и в мире // www.anti-malware.ru URL: https://www.anti-malware.ru/analytics/Market_Analysis/Enterprise_mobility_management_Russia_and_world (дата обращения 15.05.16).

REFERENCES

1 Mobile Device Management (MDM). Enterprise Mobility Management (EMM). Управление мобильными устройствами // TAdviser. ИТ-издание URL: http://www.tadviser.ru/index.php/Статья:Mobile_Device_Management_(MDM)_Управление_мобильными _устройствами_Enterprise_Mobility_Management_(EMM) (дата обращения 27.04.16).

2 Коржов В. Обзор продуктов компании ИнфоТеКС для защиты мобильных устройств // www.anti-malware.ru URL: https://www.anti-malware.ru/reviews/ViPNet_Client_for_Android_and_ViPNet_Connect (дата обращения 27.04.16).

3 Пугач О.В. Математические методы оценки рисков // Заводская лаборатория. Диагностика материалов. 2013, № 79. С. 64-69.

4 Чубуков А. Консьюмеризация в корпоративном секторе: насколько она безопасна? // www.pcweek.ru URL: http://www.pcweek.ru/security/article/detail.php? ID=138037 (дата обращения 11.05.16).

5 Ференец В. Обзор рынка управления корпоративной мобильностью (EMM) в России и в мире // www.anti-malware.ru URL: https://www.anti-malware.ru/analytics/Market_Analysis/Enterprise_mobility_management_Russia_and_world (дата обращения 15.05.16).

METHOD OF ORGANIZING THE PROTECTION OF CORPORATE INFORMATION ON MOBILE DEVICES

K.V. BRAUN, V.A. CHASTIKOVA

Kuban State Technological University,
2, Moskovskaya st., Krasnodar, Russian Federation, 350072,
e-mail: chastikova_va@mail.ru

In this article are described development prospects of the enterprise mobility and problems of information security with this trend. Since this trend is developing in Russia, the problem of protecting corporate information is very relevant. Based on the fact that the processing, storage and transmission of information on portable devices has distinctive features, some methods in different areas of information security from risk assessment prior to the planning of organizational security reviewed and adapted. New methods of calculation based on existing mathematical apparatus of the coefficients proposed and collected in the form of a detailed methodology.

Key words: information security, mobile devices, enterprise mobility, risk assessment, threat model, remote access.