АНАЛИЗ РИСКОВ ИСПОЛЬЗОВАНИЯ В КОМПАНИЯХ ТЕНЕВЫХ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ

ANALYSIS OF RISKS OF USE IN COMPANIESSHADOW CLOUD APPLICATIONS

А. В. Кулешова, A. V. Kuleshova

Аннотация: *В данной статье рассматриваются угрозы, связанные с возникновением в организации теневых облачных приложений. Производится подробный анализ возможных опасностей, результаты которого представлены в виде карты рисков. В работе также выявляются способы контроля использования в компании теневых информационных технологий, для минимизации указанных рисков.*

Abstract: *This article discusses the threats associated with the emergence of shadow cloud applications in the organization. A detailed analysis of possible hazards is made, the results of which are presented in the form of a risk map. The work also reveals ways to control use in shadow information technologies, to minimize risks.*

Ключевые слова: *риски, теневые ИТ, облачные приложения.*

Keywords: *risks, shadow IT, cloud applications.*

Эффективность практически любого современного предприятия в настоящее время довольно таки сильно зависит от эффективности его ИТ — инфраструктуры. В связи, с чем актуальным и важным является вопрос выбора используемых им приложений, в том числе из большого числа облачных сервисов.

В последнее время, в сфере информационных технологий все чаще упоминается о явлении, получившем название «Теневое ИТ». Термин «Теневые ИТ» (Shadow IT) используется для описания IT-систем и решений, развернутых и используемых в организациях без формального одобрения со стороны непосредственного руководства.

На данный момент, построение и развертывание корпоративных IT-решений, как правило, регламентируется большим количеством актов и положений, описывающих рекомендованные структуру и систему безопасности данных организации. Однако многие сотрудники, не всегда подчиняются политике безопасности компании.

Другими словами, угрозы безопасности возникают в каждом случае, когда данные или приложения свободно и неконтролируемо перемещаются через границу защищаемых систем, сетей, физического местонахождения или безопасных доменов.

Согласно отчетам исследовательской компании Gartner, специализирующейся на рынках ИТ, одним их самых распространенных нарушений безопасности компании является несанкционированное использование облачных решений [1].

Целью данной работы является анализ рисков, связанных с использованием теневых ИТ в компании.

Для достижения поставленной цели необходимо решить следующие задачи:

— выявить основные риски, связанные с использованием облачных приложений, составить карту рисков, а также отобразить графическую модель определяющую основные причины использования теневого облака в компании;

— разработать стратегию минимизации рисков, связанных с использованием теневых облачных приложений, посредством определения способов контроля использования приложений.

Для выявления рисков организаций, связанных с теневым облаком, необходимо раскрыть понятие облачных решений и проанализировать значимость конфиденциальности данных в облаке.

Под термином «облако» следует понимать организацию доступа по сети к удаленному дата-центру с оплатой за фактическое потребление вычислительных ресурсов [2].

У пользователя облачных технологий появляется возможность получить вычислительные мощности и программное обеспечение «как услугу», а это значит, что ему не нужно заботиться ни о работоспособности инфраструктуры, ни о программном обеспечении — эти обязанности теперь лежат на плечах поставщика облачных услуг.

Несмотря на все преимущества облачных приложений, существует ряд моментов, которые могут иметь негативные последствия, в особенности, если речь идет о публичных облачных приложениях. Обновление программ облачных приложений влияет на огромное количество пользователей, что может привести к серьезным авариям. Кроме того, использование облачных технологий далеко не всегда является безопасным. Облачные ресурсы играют всё большую роль в решении корпоративных ИТ — задач, а также в реализации бизнес-стратегий. По достоинству оценив возможности работы в облаке, многие сотрудники пользуются его функционалом и в обход IT-подразделений компании приобретают и используют приложения самостоятельно. [3]

К сожалению, во многих компаниях отсутствует какой-либо упреждающий подход к управлению безопасностью и соблюдению требований по обеспечению конфиденциальности и защите данных, хранящихся в облачных окружениях. В большинстве организаций в облаке находится большая часть конфиденциальной и иной критически важной информации. Зачастую в организации не проявляют должную осторожность в отношении размещения подобной информации в облачном окружении для доступа третьих лиц, например, бизнес-партнёров, подрядчиков или поставщиков.

Для выявления наиболее сильных теневых угроз и методов их

устранения, в ходе данного исследования автором был проведен анализ рисков связанных с теневыми облачными приложениями.

Для того чтобы максимально точно отобразить ситуацию, возникающую в компании при использовании теневых облачных приложений, автором был проведен анализ рисков, результаты которого оформлены посредством карты рисков.

Карта рисков — это графическое описание рисков, позволяющее выявить критически важные опасности, смягчить их и обеспечить им управление.

Построение карты рисков, как правило, проходит в несколько этапов: идентификация рисков; описание и оценка рисков; построение карты рисков; описание стратегии управления рисками.

На первом этапе, необходимо провести идентификацию рисков. Процесс идентификации рисков представляет собой выявление опасностей до того, как те или иные риски смогли неблагоприятно повлиять на организацию.

В данной работе выявление рисков проводилось при помощи следующих двух методов:

— идентификация, основанная на целях. Представляет собой анализ рисков, которые способны воспрепятствовать достижению основных целей компании;

— идентификация, основанная на систематизации. Является анализом на базе полученного ранее опыта.

В ходе исследования были выявлены следующие риски, связанные с теневыми ИТ:

- некомпетентность руководителя ИТ — службы;
- несовершенство используемой в настоящее время облачной системы;
- некомпетентность сотрудников;
- ошибочная формулировка бизнес-процессов компании;
- неконтролируемая авторизации пользователей;
- отсутствие должного контроля провайдеров облачных приложений;
- использование облачным провайдером низко бюджетных серверов;
- отсутствие разграничений доступа к данным в облаке;
- низкий контроль над учетными записями.

После выявления интересующих рисков, наступает следующий этап анализа описание и оценка выбранных рисков, осуществляемая при помощи метода «Вероятность-потери».

Шкала оценок основных параметров в используемом методе отображена в таблицах 1 и 2. На данном этапе происходит распределение рисков по виду, где каждой группе рисков присваивается определенный балл. Как, например, в таблице 1 при выявлении вероятности наступления риска «слабо вероятному» виду риска присваивается минимальный балл равный 1,а «возможному» виду риска присваивается максимальные 5 баллов.

Как видно из таблицы, при меньших баллах вероятность наступления риска крайне мала, а при более высоких баллах событие наверняка произойдет.

Далее следует оценить ущерб, который может быть нанесен организации при наступлении того или иного риска. Результаты оценки отображены в табл. 2.

После введения бальной шкалы для групп рисков, необходимо соотнести идентифицированные риски к какой либо группе, то есть присвоить каждому риску свой балл.

Для наиболее точной оценки риска были привлечены эксперты из ИТ-области, а именно руководители ИТ-компаний. Каждому эксперту была предложена анкета с выявленными в работе рисками (рис.1), в которой он, основываясь на своих знаниях и опыте, выставлял соответствующие оценки вероятности наступления риска «Р» и величины потерь от наступления риска «I».

Таблица 1

Классификация рисков по вероятности возникновения

Виды рисков	Вероятность наступления (Р)		
	Количественный подход		Качественный подход
	Pq (баллы)	Р (в долях единицы)	
Слабовероятные	1	0,0<P⩽0,1	Событие может произойти в исключительных случаях
Маловероятные	2	0,1<P⩽0,4	Редкое событие, но как известно уже имело место.
Вероятные	3	0,4<P⩽0,6	Наличие свидетельств, достаточных для предположения возможности события.
Почти возможные	4	0,6<P⩽0,9	Событие может произойти.
Возможные	5	0,9<P⩽1,0	Событие, как ожидается, произойдет.

Таблица 2

Классификация рисков по величине потерь

Виды рисков	Величина потерь	
	I (балл)	в% от плановой прибыли
Минимальные	1	0% <I⩽ 10%
Низкие	2	10% <I⩽ 40%
Средние	3	40% <I⩽ 60%
Высокие	4	60% <I⩽ 90%
Максимальные	5	90% <I⩽ 100%

На рисунке представлена экспертная оценка рисков руководителем филиала компании « АЙТИ Технологии» Кидяровым Денисом Александровичем, с опытом работы в сфере ИТ около 7 лет.

Далее, в качестве примера, следует рассмотреть заполненную экспертом форму по одному из рисков «Низкий контроль над учетными записями» в системе (рисунок 1).

Данный риск вызван злоупотреблением учетными записями бывших сотрудников или временно не используемыми записями. Таким образом возникает уязвимость с точки зрения фильтрации данных, раскрытия конфиденциальных сведений и корпоративных секретов.

Эксперт определил вероятность наступления данного риска 0,9 , величину потерь 0,7. Таким образом, риск «низкий контроль над учетными записями» соответствует группе возможных рисков (0,9 < P < 1,0):Pq = = 5 баллов. А по величине потерь принадлежит к группе высоких рисков (60% < I ≤ 90%):I = 4 балла.

Далее оценивается индекс риска: Ir = 20 баллов. Данный риск соответственно можно отнести по степени воздействия на проект как существенный, а по уровню как непереносимый.

Таким образом, результаты экспертного опроса, переведенные посредством данных табл. 1 и 2 в балльную систему оценок, представлены в табл. 3 «Описание и оценка выбранных рисков».

Как сказано выше, третьим этапом работы анализа рисков является составление карты рисков. Данный этап включает в себя размещение рисков на карту рисков на основании рангов их воздействия и ранга вероятности. Каждый риск размещается в соответствующую ячейку.

Далее необходимо определить границу толерантности к риску. На карте определяют те риски, которые требуют постоянного контроля. Те угрозы, которые находятся ниже границы, в настоящее время считаются приемлемыми, но это вовсе не означает, что ими не нужно управлять. На рисунке 2 синим цветом выделена граница терпимости к риску, риски находящиеся выше этой границе являются непереносимыми, риски отображенные ниже считаются приемлемыми.

Анализ рисков
использования теневых облачных приложений в организации

ФИО эксперта: Кудряв Денис Александрович
Место работы, должность: ООО „Айти Технологии управления проектами"
Опыт работы: 7 лет
Ученая степень: —
Ученое звание: —
Опыт участия в экспертных оценках: 2

№	Название риска	Вероятность наступления	Потери
1	Некомпетентность руководителя ИТ службы	0,9	50%
2	Несовершенство используемой в настоящее время системы	0,7	90%
3	Некомпетентность сотрудников	0,4	40%
4	Ошибочная формулировка бизнес-процессов компании	0,6	40%
5	Неконтролируемая авторизация пользователей	0,9	90%
6	Отсутствие должного контроля провайдеров облачных приложений	0,8	80%
7	Использование облачным провайдером низкобюджетных серверов	0,9	40%
8	Отсутствие разграничений доступа к данным в облаке	0,7	60%
9	Низкий контроль над учетными записями	0,9	70%

Эксперт: Дата: 16.02.2017

Рис. 1- Экспертная оценка

5	10	15 Некомпетентность руководителя ИТ службы	20 -Несовершенство используемой в настоящее время системы	25 Неконтролируемая авторизация пользователей
4	8 Использование провайдером низкобюджетных серверов	12	16 Отсутствие разграничений между личным и корпоративным доступом	20 -Низкий контроль над учетными записями
3	6	9 Некомпетентность сотрудников	12 Ошибочная формулировка бизнес-процессов компании	15 Отсутствие контроля провайдеров облака
2	4	6	8	10
1	2	3	4	5

Рис. 2 — Карта рисков использования теневых облачных приложений

Таблица 3

Описание и оценка рисков теневых облачных приложений

№	Название риска	Описание риска	Возможные последствия	Возможный Ущерб (P) баллы	Вероятность наступления (I) баллы	Индекс Риска (P*I)
1	Некомпетентность руководителя ИТ-службы	1) Отсутствие знаний об используемых приложениях. 2) В компании не проводится обучение сотрудников по информационной безопасности	Сотрудники не знают, какие облачные приложения можно использовать для безопасной работы. Неправильный выбор приложений и их небезопасное использование может привести к утечке конфиденциальных данных.	5	3	15
2	Несовершенство используемой в настоящее время облачной системы	Неудобство интерфейса или недостаточность функционала облачной системы.	Сотрудники находят более удобные приложения, которые зачастую являются небезопасными для организации.	4	5	20
3	Некомпетентность сотрудников	Сотрудники, в силу халатности и/или незнания, не правильно работают с существующей системой и не знают какие правила безопасности следует соблюдать при использовании дополнительных ресурсов.	Несоблюдение требований безопасности. Утечка данных.	3	3	9
4	Ошибочная формулировка бизнес-процессов компании	Использование систем, которые не соответствует требованиям компании по полной автоматизации основных бизнес-процессов компании	Пользователи осуществляют самостоятельный поиск приложений, способных выполнить нужные задачи.	4	3	12
5	Неконтролируемая авторизации пользователей	Доступ к конфиденциальным данным свободен для всех пользователей.	Конфиденциальной информацией владеют все пользователи системы.	5	5	25
6	Отсутствие должного контроля провайдеров облачных приложений	Отсутствие данных о местоположении провайдеров облачных приложений, и как следствие неизвестность относительно надежности центра обработки данных.	Сбои в центре обработки данных, что может привести.	4	4	16
7	Использование облачным провайдером низкобюджетных серверов	Производительность и надежность облачной платформы во многом зависят от того, какие ИТ-системы использует провайдер	Использование низкобюджетных серверов увеличивает вероятность их выхода из строя, снижает надежность и влияет на непрерывность работы сервиса.	5	3	9
8	Отсутствие разграничений доступа к данным в облаке	Облачные приложения не предполагают разграничения между личным и корпоративным использованием данных	Утечка данных из личных устройств сотрудника	4	4	16
9	Низкий контроль над учетными записями	Злоупотребление учетными записями бывших сотрудников или временно не используемых записей	Уязвимость с точки зрения фильтрации данных, раскрытия конфиденциальных сведений и корпоративных секретов	5	4	20

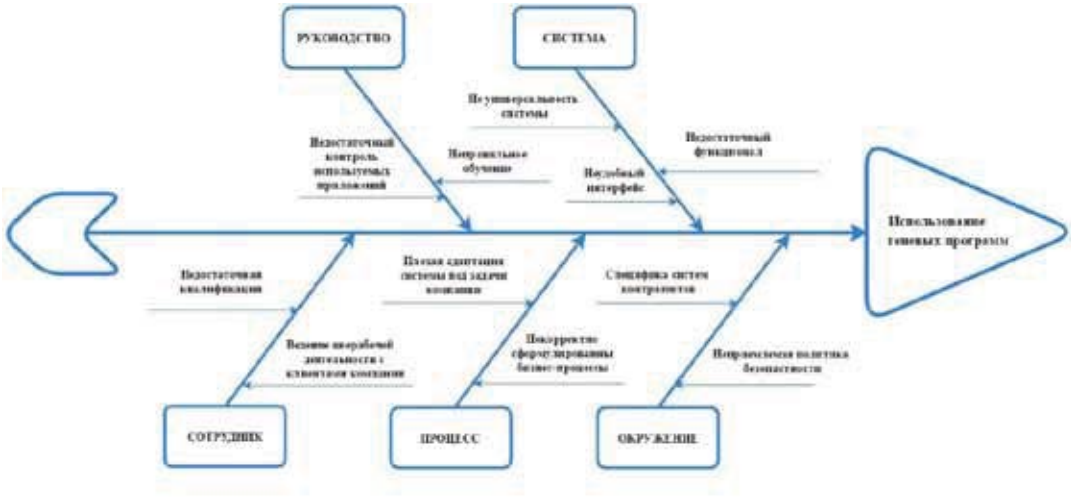

Рис. 3 — Диаграмма Исикавы «Использование теневых программ»

телей», а наименее «Использование провайдером низко бюджетных серверов». Следовательно, на первый следует обратить особое внимание.

Далее следует рассмотреть причинно-следственные связи использования теневых облачных программ при помощи графического метода — Диаграммы Исикавы. Данный метод графического анализа является инструментом для определения причин проблемы и её последующего графического представления в форме рыбной кости. Анализ диаграммы включает в себя пять основных причин, каждая из которых может быть разделена на причины следующего уровня (подробные причины), которые также могут разбиваться на другие причины [4]. Проведенный анализ представлен на рис. 3.

Как видно из рисунка, к пяти основным причинам возникновения теневых программ относятся: руководство, система, сотрудник, процесс и окружение. Наиболее важными подробными причинами являются недостаточный функционал существующей системы и плохая адаптация системы под задачи компании. Таким образом, можно сделать вывод о том, что в использовании несанкционированных приложений в компании, прежде всего, виновато ее руководство. Так как, при грамотной формулировке задач компании, значительно легче создать систему с требуемым функционалом, для работы сотрудников.

Наиболее значительную роль в контроле за теневыми облачными приложениями несет ИТ отдел компании. Согласно отчетам исследовательской и консалтинговой компании Gartner, специализирующейся на рынках ИТ к 2018 году на долю облачных приложений будет приходиться свыше 50% расходов организации. Так как многим организациям тяжело воспрепятствовать популярному в данный момент тренду «теневого облака», ИТ — отделам стоит тесно сотрудничать с другими департаментами, чтобы обеспечить компании максимум пользы при минимуме любых рисков.

К последнему этапу работы относится разработанная стратегия использования теневых облачных приложений в компании, включающая в себя способы контроля теневой деятельности сотрудников и рекомендации для своевременной реакции ИТ-отдела.

Основные способы контроля теневых приложений отображены на рис. 4.

Таким образом, представим основные рекомендации по контролю теневых облачных приложений в компании.

Во-первых, выявление информации о приобретенных сотрудниками приложениях.ИТ-отделу необходимо выяснить какие теневые приложения уже использовались в компании.

Во-вторых, оценка рисков связанных с использованием данных приложений.ИТ-отделу предстоит выявить существующие меры безопасности, применяемые в данных приложениях, определить местоположение обработки данных, узнать

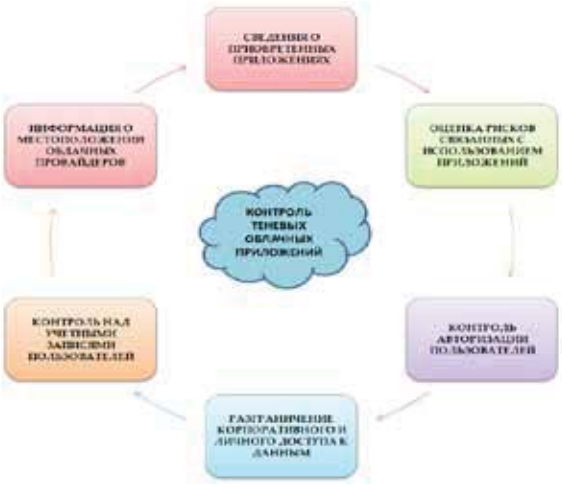

Рис.4 — Способы контроля облачных приложений в компании

о соблюдении настроек безопасности приложений в соответствии с политикой компании.

В-третьих, контроль авторизации пользователей. Компаниям стоит усилить меры защиты и ограничить круг пользователей, имеющих доступ к конфиденциальным данным.

В-четвертых, разграничение корпоративного и личного доступа к данным. Облачные приложения не предполагают разграничения между личным и корпоративным использованием данных. В целях безопасности компании необходимо ограничить копирование данных на личные мобильные устройства сотрудников.

В-пятых, усиленный контроль над учетными записями пользователей. ИТ-отделу компании следует пристально отслеживать информацию о учетных записях.Злоупотребление учетными записями бывших сотрудников или временно не используемых записей возможно в течение долгого времени. Это делает организацию уязвимой с точки зрения фильтрации данных, раскрытия конфиденциальных сведений и корпоративных секретов.

И наконец, в-шестых, получение информации о местоположении облачных провайдеров. Учитывая возможность облаков находится в любой точке мира, компании следует выбирать приложение согласно области безопасности центра обработки данных.

Итак, по результатам данной работы, стоит заметить, что на данный момент сложно воспрепятствовать современному тренду теневого облака, так как облачные приложения обладают исключительными возможностями и функционалом, что хорошо известно огромному числу сотрудников компаний. Таким образом, руководству современных компаний стоит направлять теневую облачную деятельность в «нужное русло», чтобы извлечь из нее максимум пользы. Для чего следует придерживаться четкой стратегии безопасного использования теневых облачных приложений, которая поможет использовать новые возможности, сохраняя при этом свободу выбора и обеспечивая соответствие нормативным требованиям компании.

Литература:

ЭЛЕКТРОННЫЕ РЕСУРСЫ

1. Питер Ферстбрук, Шесть принципов для повышения устойчивости цифрового бизнеса и управления рисками,//Ganter.2016//[Электронный ресурс].

2. URL: https://www.gartner.com/doc/3104129?ref=SiteSearch&sthkw=shadow%20it&fnl=search&srcId=1-3478922254 (дата обращения 14.01.2017).

3. Кулишова А. В., Захарова О. И. Поддержка принятия решений в банковской сфере на основе облачных технологий // Современные научные исследования и инновации. 2016. № 9 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2016/09/71803 (дата обращения: 17.01.2017).

4. Корчагин Ю.А. Теневая экономика России в 2014-2015 годах//Центр исследований региональной экономики, 2006-2015. — URL: http://www.lerc.ru/?part=articles&art=18&page=13 (дата обращения 29.12.16).

5. Кузьмин А.М. Диаграмма Исикавы// Центр креативных технологий. 2012// [Электронный ресурс]. URL: https://www.inventech.ru/pub/methods/metod-0019/ (дата обращения 20.01.2017).

6. Николаев А. С. Совершенствование деятельности таможенных органов Российской Федерации в системе управления рисками. // Конкурентоспособность в глобальном мире: экономика, наука, технологии. 2017. № 6-3 (51). С. 98-101 [Электронный ресурс].URL: https://elibrary.ru/item.asp?id=29731105 (дата обращения 15.01.2017).