Перспективы развития ИТ-решений в сфере ИБ для организаций малого и среднего бизнеса

В. С. Ефимов[1], email: vs.efimov@live.unecon.ru

Санкт-Петербургский государственный экономический университет

Аннотация. *Изучена статистика применения облачных сервисов в России и возникающие при их использовании угрозы. Сформулированы перспективы развития СЗИ.*

Ключевые слова: *Информационная безопасность, ИТ-решения, средства защиты информации, облачные сервисы.*

Введение

Большинство компаний из все секторов экономики переходят или уже перешли на использование облачных сервисов. Эта тенденция сохраняется уже несколько лет, но в 2020 и 2021 годах количество компаний, использующих такие решения, сильно увеличилось из-за нестабильной эпидемиологической обстановки в мире.

Периодические долгосрочные карантины не позволяют владельцам компаний вести работу в режиме «оффлайн». Больше всего в этой ситуации пострадали предприятия малого и среднего бизнеса. Из-за дороговизны и нецелесообразности использования крупных ИТ-решений, позволяющих создавать защищенную корпоративную сеть для выполнения сотрудниками своих должностных обязанностей независимо от их расположения и со своих персональных компьютеров, владельцы бизнесов столкнулись с серьезной проблемой.

В своей работе автор рассматривает проблемы информационной безопасности, возникающие при переходе малого и среднего бизнеса к удалённой работе с использованием облачных решений, и перспективы развития программных ИТ-решений в области информационной безопасности.

На данный момент времени — это особенно актуально. Как известно, сначала создаются ИТ решения, а потом СЗИ (средства защиты информации) для этого решения. Отсюда можно сделать вывод, что перспективы развития решений ИБ напрямую зависят от тенденций развития информационных технологий. Грамотная оценка возможности возникновения тех или иных уязвимостей поможет заранее перестроить систему защиты информации и сократить возможные убытки, либо избежать их вовсе.

1. Статистика киберпреступлений в России

К сожалению, увеличение частоты совершения киберпреступлений во всем мире не обошло и России. Чаще всего, мошенники совершают преступления через e-mail адреса сотрудников или их телефоны. С переходом на удаленный режим работы количество атак только возросло [1].

По данным Генпрокуратуры число атак, совершенных на ИТ-системы в 2020 году, возросло до 510,4 тысяч случаев. А за первые семь месяцев 2021 года было совершенно 320 тысяч аналогичных преступлений, что на 16% больше, чем за тот же период в 2020 году. При этом от действий злоумышленников могут пострадать не только ИТ-системы малых и средних компании, но и госорганов. Этот вывод основан на исследовании, представленном компанией «Ростелеком-Солар», в котором были проанализированы системы защиты информации в 40 госорганизациях [1].

«Вишенкой на торте» является исследование компании Check-point, в котором подсчитано среднее число на организации в неделю. С точными цифрами можно ознакомиться в таблице ниже.

Таблица

Среднее число атак на организации в неделю

	В России	В мире
Мобильные угрозы	5,9%	4,9%
Банковские угрозы	4,6%	2,9%
Криптомайнеры	10,3%	6,1%
Ботнеты	11,9%	7,6%
Инфостилеры	4,6%	2,9%

2. Перспективы развития ИБ-решений

Для более объективного отражения перспектив развития СЗИ предлагается проанализировать угрозы и риски, возникающие при использовании ранее описанных ИТ решений, но для этого необходимо лучше понимать их устройство.

Облачные сервисы разделяются на SaaS, IaaS и PaaS. Согласно [2] большую часть рынка представляет категория SaaS — 65,8%. За ней идут IaaS — 23,1% и PaaS — 11,1%.

SaaS — приложение размещено на серверах провайдера услуги, что накладывает ограничения на возможности конечно пользователя по конфигурации инфраструктуры, настройки и выбору ОС (операционной системы). Самому пользователю лишь предоставляется доступ к веб-интерфейсу, использование которого возможно практически на любой

платформе. Примерами такого сервиса являются Saleforce, Cisco WebEx от Cisco [3].

IaaS — при использовании такого сервиса все функции администрирования выполняет конечный пользователь. Ему предоставлен полный контроль над вычислительными мощностями, конфигурацией облачного сервиса и право выбирать ОС, и другие необходимые для работы сотрудников приложения. Примерами этого типа являются Cherry, Microsoft Azure и AWS (Amazon Web Services) [3].

PaaS — пользователь может самостоятельно размещать на платформе необходимые ему приложения, настраивать их, но вычислительные мощности контролируются провайдером услуги. Яркими примерами могут служить хостинги веб-приложений [3].

При этом аналитики прогнозируют дальнейший рост отрасли облачных технологий не только в России, но и во всем мире. По оценкам экспертов от Raconteur, к 2025 рост ежедневных операций с онлайн данными составит 245%, по отношению к показателям в 2020 году (рис. 1). А это, в свою очередь, увеличит объем данных, хранящихся в облачных сервисах, до 175 зеттабайт.

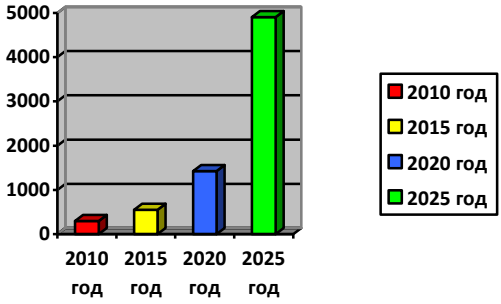

Рис. 1. Прогноз роста ежедневных операций с данными в интернете

По доступности облачные сервисы разделяют на частные облака, общественные облака, публичные и гибридные облака.

Внезависимости от типа и варианта доступности все облачные решения имеют целый ряд угроз, они существуют с самого создания облачных сервисов. Но это лишний раз подчеркивает необходимости разработки ИБ-решений способных избавить провайдеров и пользователей от «старых» угроз.

Выделяются следующие ключевые угрозы:

– кража данных;
– кража аккаунтов;
– инсайдерские атаки;
– DDOS-атаки.

Кража данных является постоянным страхом как пользователей, доверивших свою конфиденциальную информацию или персональные дынные провайдеру, так и самого провайдера. Реализация этой угрозы возможна двумя способами — физически и перехватом информации при ее передаче. Вариант проникновения злоумышленника на территорию Data-центра, оборудованного охранной системой с камерами видеонаблюдения и должным образом настроенной СКУД (система контроля управления доступом), сложно себе представить. А вот возможность перехвата информации при ее передаче вполне реальна. В связи с этим, фактически единственным, решением для малого и среднего бизнеса является использование криптографических средств защиты информации совместно с провайдером услуги. Предлагается установка «шифровальщиков» на сервера провайдера и ТС (технические средства) пользователя.

На данный момент на рынке ИБ решений имеется множество подобных готовых решений, которые подходят для малого и среднего бизнеса. Но развитие искусственного интеллекта и возможность злоумышленника использовать огромные вычислительные мощности все тех же облачных сервисов для взлома зашифрованной информации не делает этот способ защиты информации «панацеей».

Кража аккаунтов — по данным исследования, проведенного компанией Varonis [4], 43% проанализированных учетных записей пользователей облачны сервисов устарели либо не используются вовсе, что делает их легкой мишенью для злоумышленников.

Помимо этого, одна из четырех облачных учетных записей является машинной, а значит она постоянно активна и подвержена взлому круглосуточно. А программы-сканеры и службы безопасности часто игнорируют деятельность такой учетной записи из-за ее работы в фоновом режиме. И это далеко не все возможные способы реализации кражи аккаунтов, еще одни является неправильная настройка прав доступа пользователей (44% учетных записей настроены некорректно). В наше время на рынке не существует надежной защиты от этой угрозы, SIEM системы не всегда могут корректно воспринимать и обнаруживать связанные с ней уязвимости, а внутренние политики ИБ сильно подвержены «человеческому фактору».

Инсайдерские атаки — угроза способная нанести колоссальный ущерб как отдельному подразделению, так и всей организации. Эта угроза имеет множество вариантов реализации. И практически нет способов противостоять этой угрозе. Один из способов может быть ограничение прав сотрудников до минимума. SIEM-системы тоже являются решением, но даже самые современные из них все еще не могут обеспечить надежную защиту.

DDOS-атаки, на облачные сервисы могут реализовываться атаки типа «отказ в обслуживании», данный тип атак вызывает перегрузку инфраструктуры. Это приводит к трате огромных вычислительных мощностей на поддержание работоспособности системных ресурсов, из-за чего основные функции облачного сервиса становятся недоступны для пользователей решения. Перестают работать не только функции сервиса, но и в системе защиты появляются «дыры», благодаря которым злоумышленники получают доступ к конфиденциальной информации и данным учетных записей, хранящихся на серверах. Чаще всего применяются распределенные, или DDoS-атаки, но существуют и другие типы атак, которые могут нанести существенный ущерб системе. На пример, используя уязвимости в Web-сервисах или базах данных, с помощью асимметричных DoS-атак прикладного уровня злоумышленники могут «выключить» приложения с очень малой полезной нагрузкой [5]. Сила атак такого рода зависит от ресурсов вычислительных мощностей, которыми располагают злоумышленники. Не так давно это были тысячи ПК со всего мира, зараженных примитивным вирусом, но на сегодняшний день у злоумышленников есть возможность использовать несколько облачных сервисов. В таком случае вычислительные мощности можно сравнить с сотнями тысяч ПК, что ставит серьезные вопросы перед службами безопасности любого бизнеса, в том числе малого и среднего. Учитывая, что у малого и среднего бизнеса нет огромных финансовых ресурсов для создания качественной и стойкой к таким атакам системы защиты, то решением является использование межсетевых экранов. Например, решения от StormWall, AKAMAI могут сократить убытки. Помимо этого, необходимо постоянно проводить резервное копирование критически важной информации.

Стоит отметить, что упомянутые решения актуальны на данный период времени, но, с текущими темпами роста развития информационных технологий, их эффективность быстро сократится. Компаниям, использующим межсетевые экраны для защиты сетевых подключений, всегда важно помнить об этом и постоянно искать пути для совершенствования своей системы защиты.

Учитывая все вышеописанные угрозы, можно сделать вывод о том, как и в каком направлении будут развиваться ИБ-решения. Разработчикам решений по информационной безопасности необходимо внимательно следить за развитием не только облачных, но и остальных информационных технологий.

Для решения проблемы защищенности малого и среднего бизнеса от кибератак нужно развивать средства защиты сетевых подключений и особое внимание уделять доступности качественных межсетевых экранов.

Заключение

В данной статье была приведена статистика киберпреступлений в России, их направленность и специфика.

Проанализирована статистика использования облачных сервисов и тенденции их развития. Кроме этого, в работе были рассмотрены основные угрозы, возникающие при использовании облачных сервисов малыми и средними предприятиями. Также обозначены недостатки существующих методов и средств защиты информации. На основе изложенных в работе фактов выдвинуты предположения по перспективам развития средств защиты информации для малого и среднего бизнеса.

Список литературы

1. Число киберпреступлений в России [Электронный ресурс]: Статья – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BB%D0%B5%D0%BD%D0%B8%D0%B9_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8

2. Облачные сервисы (рынок России) [Электронный ресурс]: Статья – Режим доступа: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_(%D1%80%D1%8B%D0%BD%D0%BE%D0%BA_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8)

3. Яковлев М. С. Модели облачных сервисов: IAAS, PAAS, SAAS / М. С. Яковлев, Е. Н. Барашко, М. А. Шевченко // Наука и инновации в

современном мире: Сборник научных статей / Научный редактор А. Х. Цечоева. – Москва, 2020. – С. 145-147

4. Исследование рисков SaaS Varonis: 43% всех облачных учетных записей устарели, не используются и подвергаются риску. [Электронный ресурс] – Режим доступа: https://blog.varonis.ru/saas-risk-report

5. Кадыров Р. Р. Методы обнаружения и предотвращения DDOS-атак / Р. Р. Кадыров // Политехнический молодежный журнал. – 2019. – № 7(36). – С. 1.