УДК 338.49

Лебедев Дмитрий Валерьевич,
магистрант,
Кафедра анализа систем и принятия решений,
Институт экономики и управления,
ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина,
г. Екатеринбург, Российская Федерация

РАЗРАБОТКА БИЗНЕС-СИСТЕМЫ НА ОСНОВЕ АВТОМАТИЗАЦИИ ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Аннотация:
В статье представлена бизнес-модель по Остервальдеру (Business Model Canvas) по выходу на рынок информационной безопасности (далее, ИБ) с конкурентной системой класса SGRC (Security Governance, Risk management and Compliance). Даны рекомендации по реализации бизнеса в сегменте ИБ и представлены основные пункты для реализации бизнеса.

Ключевые слова:
Бизнес-модель Остервальдера, центр реагирования и мониторинга, инциденты, реагирование.

Реализация бизнеса в сфере ИБ является одним из самых критичных. Связано это с несколькими причинами.

1. Рынок ИБ имеет определенную сформированность.
2. Рынок ИБ является конкурентным и в большинстве сегментах рынка нет явно сформированных лидеров.
3. Системы по ИБ являются критичными для стабильности бизнеса, и миграция с одного решения на другое считается нежелательным процессом.

Однако в ИБ есть определенная проблема, которая заключается в постоянном росте инцидентов ИБ и соответствующем росте потерь для бизнеса от реализации данных инцидентов. Согласно отчету Positive Technologies за 2022 год общее количество инцидентов ИБ увеличилось на 20,8% по сравнению с 2021 годом. В 2020 году рост киберинцедентов составил 51%, а в 2021 – всего 6,5% [1, 2, 3]. На рисунке 1 представлен график по количеству инцидентов в 2019, 2020, 2021 и 2022 годах (по кварталам).

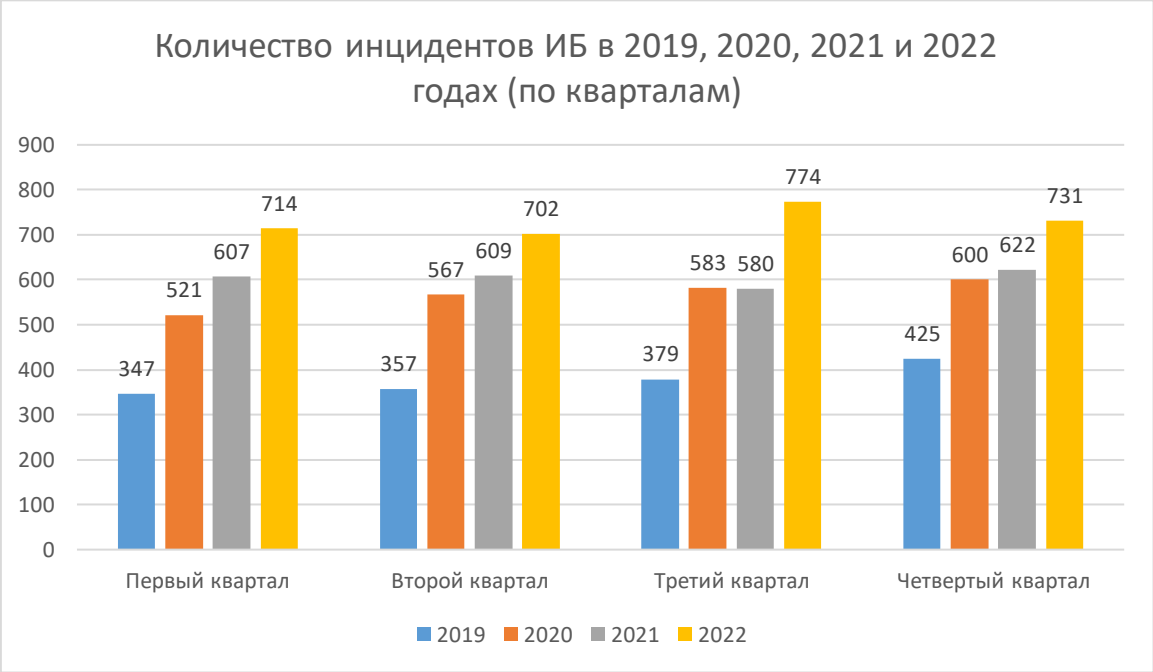

Рисунок 11 – Количество инцидентов ИБ в 2019, 2020, 2021 и 2022 годах по кварталам

Таким образом к вопросу обеспечения ИБ требуется подходить систематически, опережая рост уровня угроз возможностями автоматизированного либо автоматического реагирования. Соответствующая реализация бизнеса в области ИБ должна удовлетворять данным потребностям и иметь конкурентные преимущества.

Далее в статье продемонстрированы лучшие практики по реализации бизнеса в сегменте ИБ с помощью бизнес-модели Остервальдера.

Одним из вариантов автоматизации процессов управления ИБ на предприятии являются системы класса SGRC (Security Governance, Risk management and Compliance). Основной функционал данных систем:

1. модуль управления информационными активами, стандартами и документами по ИБ (Governance);
2. модуль управления рисками (Risk management);
3. модуль управления соответствием требованиям законодательства.

Данный рынок в Российской Федерации является представляется следующими системами:

1. ePlat4m от компании ООО «Кит.р»
2. R-Vision от компании ООО «Р-ВИЖН»
3. Security Vision от компании ООО «Интеллектуальная безопасность»
4. Securitm от компании ООО «Секъюритм»

Системы класса SGRC относятся к сегменту SOC+. К данному рынку относятся вендоры, которые производят системы для функционирования центра мониторинга ИБ. Перечень систем для рынка SOC+:

- IRP (Incident Response Platform) – платформа реагирования на инциденты, представляет собой автоматизацию и роботизацию SOC;
- SGRC;
- TIP (Threat Intelligence Platform) – платформа для организации проактивного реагирования на киберугрозы, которая позволяет собирать информацию из различных источников, накапливать ее, обогащать и обрабатывать.
- SOAR (Security Orchestration Automation and Response) – системы оркестрации, автоматизации и реагирования, которые применяются для автоматизации процессов расследования инцидентов ИБ и принятия контрмер по ним;
- CAASM (Cyber Assets Attack Surface Management) – система управления поверхностью кибератак за счет сканирования информационных активов предприятия

Объем рынка SOC+ представлен на рисунке 2. Финансовые показатели вендоров, которые разрабатывают в том числе систему класса SGRC представлен в таблице 1 [4, 5, 6]. Причем, ООО «Секъюритм» производит только систему класса SGRC. Все остальные компании имеют ряд других систем для рынка SOC+.

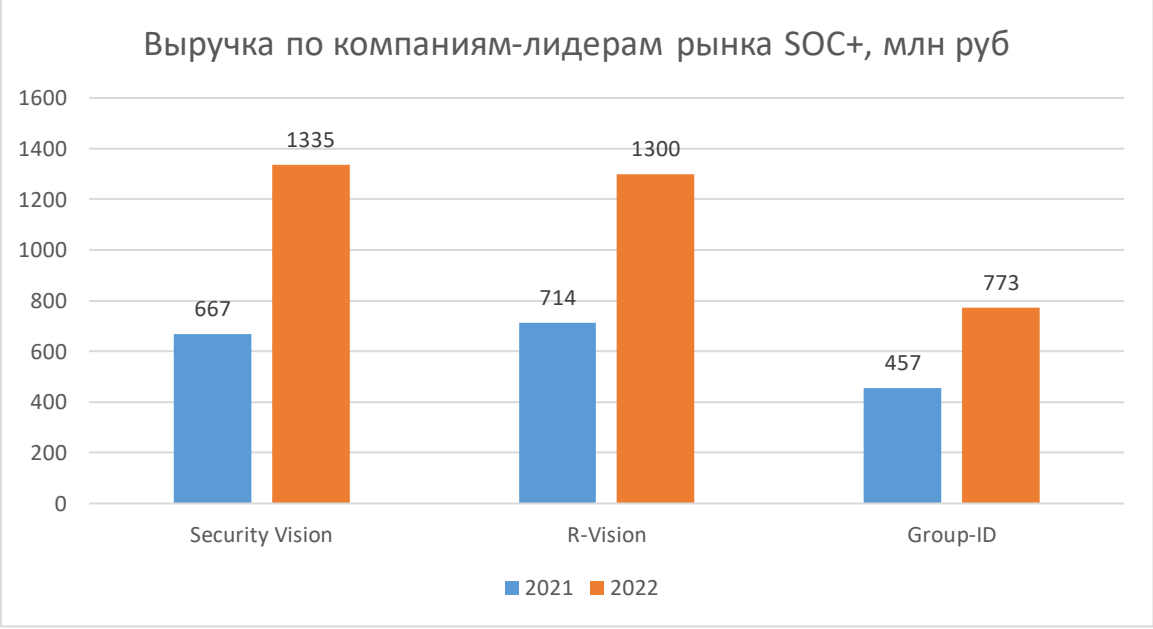

Рисунок 12 – Выручка по компаниям-лидерам рынка SOC+

Таблица 1 – Финансовые показатели вендоров рынка SOC+

Вендор	**Выручка, млн рублей**		**Чистая прибыль, млн рублей**	
	2021	**2022**	**2021**	**2022**
ООО «Секъюритм»	0,625	3,7	0,275	1,6
ООО «Р-ВИЖН»	714,3	1 300,0	183,9	523,5
ООО «Интеллектуальная безопасность»	667,4	1 335,0	нет данных	нет данных
ООО «Кит.р»	280,3	262,6	276,1	246,8

Таким образом видно, что данный рынок является сформированным. Поэтому реализация бизнеса в данном сегменте имеет определенные риски, связанные с конкуренцией.

Однако, даже на конкурентных рынках, есть возможность зайти с новой системой. Эта возможность заключается в реализации конкурентного функционала, отсутствующего на данном рынке. Но даже если выйти на существующий рынок с системой с конкурентным функционалом переход заказчиков на данную систему является весьма проблемным из-за критичности миграции и, в любом случае, присутствующей конкуренции.

Поэтому, для рынка ИБ предлагается первоначальный выход на рынок только с наличием конкурентного функционала и, возможно, другим позиционированием самой системы. С учетом того, что на рынке отсутствует конкурентноспособный функционал, покупка данной системы не повлияет на «болезненность» перехода заказчика с одной системы на другую. Однако, развитие дальнейших модулей, которые и являются функционалом SGRC, позволит осуществить переход заказчика с одной системы на другую с учетом уровня доверия к изначально реализованному конкурентноспособному функционалу. Таким образом будет обеспечиваться «легкость» миграции.

Например, для систем класса SGRC таким конкурентным функционалом может стать отдельный модуль управления кибератаками. Таким образом, первоначальное позиционирование данного модуля никак не будет пересекаться с позиционированием систем класса SGRC, и позволит получить определенное доверие на рынке.

В таблице 2 показана пример бизнес-модели Остервальдера для реализации данной системы.

Данный шаблон бизнес-модели позволяет сформировать концепцию по реализации бизнеса в сегменте ИБ.

Таблица 2 – Бизнес-модель

<table>
<tr>
<td rowspan="2">Ключевые партнеры
• Организаторы профильных ИБ-конференций (изначально)
• Системные интеграторы (изначально)
• Дистрибьюторы (в дальнейшем, дополнительно)
• Аутсорсинг (управление финансами)</td>
<td>Ключевые виды деятельности
• Процессы развития (Разработка новых технологий и услуг, управление финансами)
• Основные процессы (Разработка системы; договор на продажу; доставка ПО заказчику, внедрение системы; оказание технической поддержки)
• Вспомогательные процессы (ИТ-обеспечение, юридическое обеспечение, управление персоналом, маркетинг</td>
<td rowspan="2">Ценностные предложения
Наш продукт помогает предприятиям, которые хотят своевременно реагировать и предотвращать инциденты ИБ (кибератаки), тем, что позволяет прогнозировать и визуализировать действия злоумышленников (хакеров) и предоставляет мероприятия по устранению доступных векторов атак (в отличии от конкурентов, которые предлагают только перечень защитных мероприятий).</td>
<td>Отношения с клиентами
Удержание для регулярного сотрудничества (техническая поддержка и продление)</td>
<td rowspan="2">Потребительские сегменты
• Банковский сектор
• Промышленность
• Телекоммуникации и ИТ
• Государственный сектор
• Здравоохранение
• Образование и наука
• Транспорт</td>
</tr>
<tr>
<td>Ключевые ресурсы
• Персонал
• Материальные ресурсы (заработная плата, капитальные вложения (компьютерная техника), налоги)</td>
<td>Каналы сбыта
• Выступление на профильных ИБ-конференциях – полезно для начального выхода на рынок
• Партнерство с системными интеграторами – полезно для распространения информации о системе по рынку
• Партнерство с дистрибьюторами (в дальнейшем)</td>
</tr>
<tr>
<td colspan="3">Структура расходов
• Заработная плата
• Отчисления на социальные нужды
• Капитальные вложения (компьютерная техника)
• Затраты на маркетинг
• Затраты на аутсорсинг</td>
<td colspan="3">Потоки доходов
• Упрощенная схема: Итоговая стоимость система фиксированная. Дополнительно к стоимости системы заказчик должен покупать техническую поддержку и обновление для баз модуля прогнозирования (со второго года владения)
• Продвинутая схема: каждый модуль лицензируется отдельно. Лицензии можно приобрести по отдельности или все вместе. Лицензия приобретается ежегодно или один раз на все время</td>
</tr>
</table>

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Positive Technologies. Исследования. Аналитика. Актуальные киберугрозы: итоги 2022 года. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/, свободный. (дата обращения 04.10.2023)
2. Positive Technologies. Исследования. Аналитика. Актуальные киберугрозы: итоги 2021 года. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/, свободный. (дата обращения 04.10.2023)
3. Positive Technologies. Исследования. Аналитика. Актуальные киберугрозы: итоги 2020 года. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/, свободный. (дата обращения 04.10.2023)
4. Государственный информационный ресурсы бухгалтерской (финансовой) отчетности. [Электронный ресурс]. – Режим доступа: https://bo.nalog.ru/, свободный. (дата обращения 13.10.2023)
5. РБК Компании. Security Vision. [Электронный ресурс]. – Режим доступа: https://companies.rbc.ru/id/5157746309518-security-vision/#finance, свободный. (дата обращения 13.11.2023)
6. CISOCLUB. интервью с экспертами по информационной безопасности. Интервью с Security Vision. Итоги 2022 года, планы на 2023 год. [Электронный ресурс]. – Режим доступа: https://cisoclub.ru/intervju-s-security-vision-itogi-2022-goda-plany-na-2023-god/, свободный. (дата обращения 13.11.2023)

Lebedev Dmitry Valerievich,
Master student,
Department of Systems Analysis and Decision-Making,
Graduate School of Economics and Management,
Ural Federal University named after the First President of Russia B.N. Yeltsin,
Yekaterinburg, Russian Federation

DEVELOPMENT OF A BUSINESS SYSTEM BASED ON AUTOMATION OF INFORMATION SECURITY MANAGEMENT PROCESSES

Abstract:
The article presents the Business Model Canvas for entering the information security market with a competitive SGRC (Security Governance, Risk management and Compliance) class system. Recommendations on the implementation of business in the information security segment are given and the main points for the implementation of business are presented.

Keywords:
Business Model Canvas, Security Operation Center, incidents, response.