Секция «Социальные технологии и менеджмент»

Информационные риски функционирования современных организаций

Научный руководитель – Юрасова Мария Владимировна

Швыряев Павел Сергеевич
Студент (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Социологический факультет, Кафедра социологии организаций и менеджмента, Москва, Россия
E-mail: pavel71.shvyryaev@gmail.com

В исследовании предпринята попытка проанализировать, классифицировать и систематизировать информационные риски функционирования организаций в постиндустриальном обществе.

Метод исследования - кейс-стади. Данный метод, по мнению автора, является одним из наиболее продуктивных методов исследования по выбранной теме, поскольку проявлением тех информационных рисков, которые имеются в современных организациях, являются конкретные случаи наступления, например, сбоев или утечек информации, которые часто получают широкое освещение в СМИ.

Для проведения исследования был подготовлен список событий, каждое из которых было подвергнуто детальному анализу в рамках кейс-стади. Критерии, по которым был подготовлен список событий:

1. Событие являлось проявлением тех информационных рисков, которые характерны для современных постиндустриальных организаций.
2. Событию должно быть не более восьми лет: с 1 января 2012 по 1 января 2020 года.
3. Упоминания о событии в новостных сводках СМИ.
4. Неоднородность списка: в основе событий были разные причины, по которым они наступили.

На основании вышеизложенных критериев, был подготовлен следующий список событий, каждое из которых было подвергнуто детальному анализу по методу кейс-стади:

1. Утечка персональных данных клиентов Сбербанка в октябре 2019 года [1].
2. Утечка персональных данных клиентов Альфа-банка в ноябре 2019 года [2].
3. Сбой в работе соцсети “ВКонтакте” в результате пожара в дата-центре в ноябре 2019 года [3].
4. Массовое заражение компьютеров вирусом WannaCry в мае 2017 года [4].
5. Обнаружение критической ошибки в операционной системе VxWorks в августе 2019 года [5].
6. Потеря компанией Knight Capital Group 440 миллионов долларов из-за некорректного релиза программного обеспечения в августе 2012 года [6].
7. Принятие закона о “Суверенном интернете” [7].

Результаты исследования

По результатам исследования была подготовлена результирующая таблица с классификацией информационных рисков постиндустриальных организаций:

1. Технологические: некорректно функционирующее программное обеспечение. Например, обнаружение критической ошибки в операционной системе VxWorks.
2. Инфраструктурные: сбои и неполадки в работе инфраструктуры в результате природных и техногенных катастроф. Например, сбой в работе соцсети “ВКонтакте” в результате пожара в дата-центре.

3. Безопасности: кража данных, заражение вредоносной программой. Например, утечка персональных данных клиентов Сбербанка.

4. Риски политического и правового характера: политика государства в области в области цифровых технологий. Например, принятие закона о “Суверенном интернете”.

5. Человеческого фактора: сбой по причине невнимательности или отсутствия соответствующей квалификации у персонала. Например, потеря компанией Knight Capital Group 440 миллионов долларов из-за некорректного релиза программного обеспечения.

Также на основании проведенного исследования были составлены следующие классификации информационных рисков:

1. По степени воздействия на бизнес-процессы организации.
2. По вероятности возникновения.
3. По возможности управления рисками.
4. По характеру последствий на организацию.

По степени воздействия на бизнес-процессы организации можно выделить следующие уровни риска:

1. Критический - в результате произошедшего инцидента процессы внутри организации полностью парализованы.

2. Высокий - в результате сложившейся ситуации организация осуществляет свою деятельность с серьезными отклонениями от нормы, или же с ограничениями.

3. Средний - в результате инцидента затронут модуль или процесс, не являющийся для организации критическим и не оказывающий воздействия на базовые модули организации.

4. Низкий - некритичным образом затронут сопутствующий модуль или процесс внутри организации, не оказывающий воздействия на достижение организацией своих целей.

По вероятности возникновения можно выделить следующие виды рисков:

1. Высокая вероятность: инцидент возникает не реже одного раза в две недели.

2. Средняя вероятность: инцидент возникает не чаще раза в месяц, но не реже двух раз в год.

3. Низкая вероятность: инцидент возникает не чаще раза в год.

По возможности управления рисками можно выделить следующие виды:

1. Легкоуправляемые: организация способна собственными силами минизировать риск проявления данного риска в будущем. Например, минимизировать риск появления критичной ошибки в программе можно за счет деятельности специалистов по качеству (QA) или написания автоматических тестов.

2. Трудноуправляемые: вероятность проявления данного риска высока, организация не имеет или практически не имеет рычагов воздействия на данный риск. Например, воздействие техногенных или природных сил на ИТ-инфраструктуру организации.

По характеру последствий для организации:

1. Репутационные: в результате инцидента пострадала репутация организации. Например, утечка персональных данных клиентов Сбербанка.

2. Потеря данных: безвозвратная потеря данных, в результате чего организация парализована. Например, случайное удаление базы данных по причине человеческого фактора.

3. Потеря денежных средств: характерно для финансово-технических компаний, когда в результате программной или человеческой ошибки происходит совершение некорректных финансовых операций. Например, потеря компанией Knight Capital Group 440 миллионов долларов из-за некорректного релиза программного обеспечения.

4. Урон для аппаратного обеспечения: в результате воздействия техногенных или природных сил аппаратное обеспечение выходит из строя. Например, сбой в работе соцсети

“ВКонтакте” в результате пожара в дата-центре.

5. Воздействие на бизнес-процессы: инцидент оказал воздействие на процессы внутри организации, вплоть до полной парализации ее функционирования. Например, в результате деятельности компьютерного вируса были заражены рабочие компьютеры сотрудников

Источники и литература

1) Горячева В., Солдатских В. Клиенты Сбербанка попали на черный рынок [Электронный ресурс]. Сайт “Коммерсантъ”, 2019. URL: https://www.kommersant.ru/doc/4111863?from=main_1 (дата просмотра: 09.02.2020).
2) Данные клиентов Альфа-банка утекли в Сеть [Электронный ресурс]. Сайт РБК, 2019 год. URL: https://www.rbc.ru/finances/07/02/2020/5e3d83589a794763b287847a. (дата обращения: 09.02.2020).
3) Российские пользователи "ВКонтакте" сообщают о сбоях в работе социальной сети [Электронный ресурс]. Сайт “ТАСС”, 2019 год. URL: https://tass.ru/obschestvo/7077695 (дата обращения: 09.02.2020).
4) Эксперты оценили ущерб от вируса WannaCry в $1 млрд [Электронный ресурс]. Сайт “RuNews24”, 2017 год. URL: https://runews24.ru/internet/25/05/2017/3deb290a821bd12cc946653ea418e439 (дата обращения: 09.02.2020).
5) Pascal Ackerman. Other attack scenarios // Industrial Cybersecurity. Efficiently secure critical infrastructure systems. — Birmingham: Packt Publishing, 2017. — P. 174.
6) Бирюков В. Ошибка программы-робота обошлась биржевому брокеру Knight в $440 млн [Электронный ресурс]. Сайт “РИА Новости”, 2012 год. URL: https://ria.ru/20120803/715752871.html (дата обращения: 09.02.2020).
7) В России вступил в силу закон о "суверенном рунете". Но работать он пока не будет [Электронный ресурс]. Сайт BBC, 2019 год. URL: https://www.bbc.com/russian/news-50259217. (дата обращения: 09.02.2020).