Муратова Эльвина Венеровна,
ФГБОУ ВО «Уфимский государственный
нефтяной технический университет»
г. Уфа, Республика Башкортостан

Научный руководитель:
Козлова Юлия Борисовна, к.с.н., доцент,
ФГБОУ ВО «Уфимский государственный
нефтяной технический университет»
г. Уфа, Республика Башкортостан

РОЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СВЯЗЯХ С ОБЩЕСТВЕННОСТЬЮ

Аннотация. Правильная информационная политика компании поможет избежать многих кризисов, в частности репутационного, который, зачастую имеет самые серьезные последствия для жизни компании

Ключевые слова: информационная безопасность, киберпреступность, защита от утечки информации.

В нынешних реалиях информационная безопасность становится не просто идеей обезопасить свои данные, а необходимостью. Информационная безопасность, или ИБ, — это мер, по защите информации от неавторизированного доступа, разрушения, модификации, раскрытия и задержек в доступе [1]. В информационную безопасность часто включают кибербезопасность.

Современный мир все больше и больше погружается в виртуальный мир. Пандемия только ускорила виртуализацию. Организации перешли на удаленный формат работы, рост популярности интернет магазинов, различных доставок, онлайн-мероприятий, мобильных банков. Через все эти каналы проходят огромное количество данных, которых люди привыкли не замечать, так как это персональные данные. Наши имена, документы, платежные карты, коммерческие тайны. Все это хранится на разных носителях, защищают которые отнюдь не решетки на окнах и металлические двери.

По исследованиям компании Positive Technologies количество кибер –атак растет с каждым годом[2]. Если в 2017 были зафиксированы 985 атак, то в 2021 году их стало 2418. Притом, что изначально целенеправленные атаки составляли 43 %, то к сейчас они выросли 74%. Последствия атак выходят за пределы отдельных компаний и влияют на целые отрасли. В прошлом году годовой ущерб от кибер-атак составил 6 трлн долларов, не учитывая репутационные риски, что для бизнеса может привести к огромному кризису.

Традиционно в топе жертв кибер-атак лидируют государственные учреждения, далее следуют промышленные предприятия, организации связанные с наукой и образованием, медицина и транспорт. Данные организации не считая важных государственных и коммерческих тайн, имеют огромные базы персональных данных. Злоумышленники могут не только вывести из строя инфраструктуру организации, но и продать украденные персональные данные.

Это приведет не только простою компании, следовательно, потерю прибыли, но и повлечет за собой репутационный кризис, понижение лояльности потребителей, уход многих клиентов к конкурентам. И выход из данной кризисной ситуации для PR-специалистов будет достаточно тяжелым.

[1] Васильева О.М., Хлебников Р.С. Информационная безопасность в организации Р.С. //Экономика и качество систем связи,2018 - №4 – С. 46

[2] Исследование Positive Technologies https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2022-rus.pdf (Дата обращения 20.11.2022)

Поэтому для предотвращения репутационного кризиса надо в первую очередь провести аудит информационной безопасности. Из данного анализа следует составить корпоративную политику и бюджет для информационной безопасности для обеспечения защиты информации. Условно информационную безопасность можно разделить на две части : внутреннюю и внешнюю. К внешней можно отнести различные программные обеспечения, которые будут защищать компанию от кибер-атак снаружи. К внутренней части относят сотрудников компании и корпоративные устои, регламенты об информационной безопасности. Значительный процент утечек информации составляют инсайдеры, чаще всего это сотрудники компании, которые не подозревают или не знали правил информационной безопасности.

В некоторых компаниях для предотвращения утечек и контролем эффективности работников используют DLP-системы. Компания Falcongaze, специализирующееся на изготовлении данного программного обечпечения, расшифровывает их так: «DLP-система (от англ. Data Leak Prevention) - это специализированное програмное обеспечение, которое защищает организацию от утечек данных. Данная технология – это не только возможность блокировать передачу конфиденциальной информации по различным каналам, но и инструмент для наблюдения за ежедневной работой сотрудников, который позволяет найти слабые места в безопасности до наступления инцидента [3]». В судебной практике уже наблюдаются инциденты, где благодаря данным системам удалось предотвратить большие утечки корпоративной информации, и избежать репутационного кризиса [4].

Однако не каждая компания может позволить себе DLP-системы для контроля сотрудников. Препятствиями могут служить не только бюджет, но и этическая сторона вопроса. Так как DLP изначально выполняет функции полного мониторинга работы сотрудника, к этому можно отнести видео-наблюдение действий на рабочем столе компьютера, историю браузера, общение в мессенджерах, а также записывание разговоров и использование веб-камеры компьютера. Не каждый сотрудник согласиться на такие условия и не каждое руководство согласиться проводить такую политику. И если в больших корпорациях, использование DLP оправданно, то в среднем и малом бизнесе это может принести неоправданные расходы. Поэтому для подобных организаций следует использовать собственные регламенты для предотвращения утечек информации и пользоваться программным обеспечением защищающих от кибер-атак извне.

Наличие средств защиты информации является отличным преимуществом в нынешних реалиях. Позволяя чувствовать в безопасности не только себя, но и клиентам компании можно сильно повысить лояльность и увеличить LTV, что особенно важно в B2B-сегменте.

Таким образом, мы рассмотрели какую роль играет информационная безопасность в связях с общественностью. Правильная информационная политика компании поможет избежать многих кризисов, в частности репутационного, который, зачастую имеет самые серьезные последствия для жизни компании. Информационная безопасность ещё только закрепляется в России, и использование её для привлечения новых и поддержки существующих клиентов является новым малоиспользуемым конкурентным преимуществом. Исходя из этого мы также можем сделать вывод что информационная безопасность нужна не только как способ защитить свою организацию от утечек информации и кибер-атак, но для создания и поддержания имиджа клиентоориентированной и «безопасной» организации.

Список литературы:

1. Васильева О.М., Хлебников Р.С. Информационная безопасность в организации Р.С. //Экономика и качество систем связи,2018 - №4 – С.46-49

[3] Определение DLP –систем URL : https://falcongaze.com/ru/pressroom/publications/dlp-sistemy/what-is-dlp.html (дата обращения – 225.11.2022).

[4] Отсылки к судебным делам URL: https://www.securitylab.ru/blog/personal/80na20/316247.php (дата обращения – 26.11.2022).

2. Грошева Е.К., Невмержицкий П. И., 2017 Информационная безопасность: современные реалии // Бизнес-образование в экономике знаний, 2017. – № 3. – С. 36.
3. Определение DLP – систем URL: https://falcongaze.com/ru/pressroom/publications/dlp-sistemy/what-is-dlp.html (дата обращения – 25.11.2022).
4. Отсылки к судебным делам URL: https://www.securitylab.ru/blog/personal/80na20/316247.php (дата обращения – 26.11.2022).
5. Исследование Positive Technologies https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/positive-research-2022-rus.pdf (Дата обращения 20.11.2022)