Секция «Риски и методы воздействия на риск в условиях цифровизации»

Управление рисками кибербезопасности в условиях современной экономики

Научный руководитель – Кленова Татьяна Владимировна

Харсеева Анастасия Юрьевна

Студент (бакалавр)

Волгоградский государственный университет, Волгоград, Россия

E-mail: axarseeva@mail.ru

В век, когда цифровые технологии распространены как в производстве, так и в повседневной жизни людей, стоит задуматься о безопасности данных, находящихся в электронном виде. Цифровые технологии - это система, позволяющая решать разнообразные задачи за короткие отрезки времени с помощью разных способов кодирования и трансляции информационных данных. Кибербезопасность - действия, направленные на защиту Интернет-сетей, программ от цифровых атак. Обычно кибератаки проводятся с целью получения доступа к конфиденциальной информации, ее изменения, вымогательства денег у пользователей, уничтожения данных, нарушения бизнес-процессов.

Существуют различные риски, которые могут повлиять на экономические процессы, но можно сказать, что риски, связанные с кибербезопасностью, наиболее распространены и являются прямой угрозой для стабильности процессов, протекающих в бизнесе. К примеру, количество атак во II квартале 2020 года выросло на 9% по сравнению с I кварталом 2020 года (наибольшее число атак пришлось на разгар пандемии COVID-19) и на 59% по сравнению со II кварталом 2019 года, следует из отчета Positive Technologies [2]. По оценкам Всемирного экономического форума, потери мировой экономики от кибератак составили в 2019 году 2,5 трлн. долларов, а к 2022 г. они могут достичь 8 трлн. долларов [1]. Плюс ко всему, рост киберпреступности подтверждается статистикой Генпрокуратуры РФ, причем произошел он исключительно за счет мошенничества с использованием электронных и цифровых средств.

Риски кибербезопасности можно считать рисками техническими, которым могут уделять мало внимания, так как в предприятии может недооцениваться их влияние на бизнес. Однако усилия для устранения подобных рисков должны прилагать не только работники IT-подразделения предприятия, но и высшее руководство, так как для предотвращения и ликвидации проблем нужно правильно направлять людей и контролировать все происходящие процессы. Влияние начальства позволит смягчить негативные последствия кибератак или свести их к минимуму.

Чтобы контролировать ситуацию, возникающую на почве рисков в связи с оцифровыванием различных процессов и данных, предприятия должны обеспечивать высокую информационную безопасность. В настоящее время нужно не только решать проблемы по мере их поступления, но и проводить профилактические мероприятия, с целью предупреждения и исключения неприятных инцидентов. Существует три основные цели, которые нужно учитывать при управлении рисками кибербезопасности: конфиденциальность (ограничение доступа для защиты конфиденциальности информационного контента); целостность (ограничение прав на изменение информации для обеспечения её достоверности); доступность (гарантированный доступ к информации для определённого круга лиц).

Стоит понимать, что в современном мире происходят постоянные изменения и совершенствования в сфере IT-технологий, но, даже несмотря на высокие темпы развития, злоумышленники всё чаще пытаются украсть данные или внедриться в производственные

процессы. Поэтому очень важно обеспечить оперативное выявление попыток несанкционированного доступа к данным и разработать эффективный план по защите и восстановлению информации. Однако предприятия могут столкнуться с различными проблемами при создании защитных средств для управления рисками кибербезопасности. К примеру, недостаточное количество квалифицированных сотрудников и незнание в сфере кибербезопасности среди всех работников, отсутствие денежных средств и т.д.

Если обратиться к примерам из жизни, становится понятно, насколько важно управление рисками кибербезопасности. В начале 2019 года было совершено несколько кибератак на крупные промышленные предприятия. Например, Norsk Hydro (производитель алюминия) частично перевел в ручной режим рабочие процессы и приостановил несколько заводов из-за кибератаки, которая привела к шифрованию файлов в инфраструктуре заводов и филиалов компании по всему миру. Принесённый ущерб оценили в 41 млн. долларов. В атаке использовался шифровальщик LockerGoga, который также был выявлен в начале 2019 года в атаках на три химические компании в США. В июне 2019 кибератаке подвергся производитель авиационных деталей ASCO, которому из-за восстановительных работ пришлось отправить домой на неопределённое время примерно 1400 сотрудников [3].

То есть, если управление рисками кибернетики будет слабым или его не будет вовсе, с большой вероятностью пострадает финансовая составляющая предприятия, возможно временное или даже полное прекращение работоспособности подразделений или предприятия в целом, банкротство, высвобождение рабочей силы, потеря репутации компании. В случае утечки конфиденциальной информации возможно обнародование персональных данных клиентов или раскрытие технологий компании, являющихся коммерческой тайной.

Итак, можно сказать, что проблема управления рисками кибербезопасности действительно существует и важна в настоящее время. Чтобы успешно бороться с киберпреступниками, руководству предприятий необходимо выделять из бюджета средства для создания надёжной защиты баз данных, бизнесс-процессов. Также важно направить денежные вложения на развитие кадрового потенциала организации, чтобы увеличить осведомлённость сотрудников о кибератаках и повысить квалификацию IT-отдела. Новые знания работников позволят своевременно выявлять попытки несанкционированного доступа к конфиденциальной информации, предотвращать попытки взлома электронных баз данных, а также помогут сократить или исключить финансовые, технические риски и риски банкротства из-за киберпреступлений.

Источники и литература

1) Киберпреступность переросла в пандемию // www.vedomosti.ru URL: https://www.vedomosti.ru/forum/technologii_novoj_realnosti/columns/2020/12/02/849244-kiberprestupnost (дата обращения: 02.03.2021).

2) Статистика кибератак: преступники предпочитают «цифру» // www.angaratech.ru URL: https://www.angaratech.ru/press-center/novosti/statistika-kiberatak-prestupniki-predpochitayut-tsifru_1198/ (дата обращения: 02.03.2021).

3) Обзор: самые громкие инциденты безопасности в 2019 году // habr.com URL: https://habr.com/ru/company/pt/blog/492778/ (дата обращения: 01.03.2021).