Секция «Управление рисками и страхование: новые вызовы и возможности»

Управление рисками кибербезопасности в современных условиях: статистика, прогнозы.

Научный руководитель – Кленова Татьяна Владимировна

Харсеева Анастасия Юрьевна
Студент (бакалавр)
Волгоградский государственный университет, Волгоград, Россия
E-mail: axarseeva@mail.ru

Цифровые технологии в настоящее время распространены во всех сферах жизни человека. Чтобы обеспечить бесперебойную работу всех процессов, протекающих в экономике, бизнесе, обычной жизни людей, необходимо уделять внимание рискам кибербезопасности. Важность киберрисков особенно проявилась в период пандемии COVID-19. С каждым днем управление киберрисками становится сложнее, так как хакеры постоянно совершенствуют свои подходы к взломам, проводимым атакам. В итоге обеспечение кибербезопасности данных заняло очень важное место, и сейчас это одна из самых обсуждаемых тем.

Последние несколько лет нагрузка на цифровые сервисы и технологии стремительно растёт. Распространение интернета составило 62,5 % от общей численности населения мира (по отчету Digital 2022 Global Overview Report). По данным аналитиков, количество интернет-пользователей за 2021 год выросло на 192 миллиона (4,0%) [1]. При этом по данным компании информационной безопасности Check Point Software Technologies, число кибератак в 2021 году выросло на 40% по сравнению с 2020 годом [3]. В России количество таких атак увеличилось на 54%. В среднем, каждую неделю хакеры совершали 1153 кибератаки.

По данным специалистов Chek Point Research видно, что в 2021 году в мире в среднем каждая 61-я организация подвергалась воздействию программ-вымогателей еженедельно (на 9% больше, чем в 2020 году). На первом месте - сектор ISP/MSP (Провайдеры Интернет и ИТ услуг), где каждая 36-я организация сталкивалась с атаками программ-вымогателей (на 32% больше, чем в 2020 году), на втором месте - сфера здравоохранения (каждая 44 организация подвергалась атакам программ-вымогателей, рост на 39% по сравнению с 2020 годом), далее - поставщики ПО (каждая 52-я организация, рост на 21%) [3].

Инновации в сфере облачных решений позволили организациям повысить гибкость бизнеса и сократить расходы, но они также открыли киберпреступникам новые возможности для совершения атак, сообщают аналитики IDC.

Хакеры применяют много различных способов, чтобы добыть конфиденциальную информацию или внедриться в бизнесс-процессы и экономику страны, что актуализирует задачу эффективного управления рисками кибербезопасности.

- Фишинг - атаки с использованием электронной почты (рассылка писем с вредоносными ссылками и программами, которые пользователь открывает на своем устройстве).
- Программы-вымогатели (ransomware) - вредоносное ПО, блокирующее доступ пользователей к их программному обеспечению и данным в системе и требует заплатить выкуп.
- Вредоносное ПО - программы, останавливающие или замедляющие работу устройств (программы-шпионы, вирусы, черви, программы-вымогатели и трояны).

- Утечки данных - метод кражи конфиденциальной информации пользователя или компании путем шпионажа или сливов за деньги.
- DDoS - атаки или отказ в обслуживании - хакеры направляют большой объем трафика к системе или серверу, заставляя его остановить или приостановить работу.
- MitM - перехват и изменение электронных сообщений с использованием поддельной точки доступа Wi-Fi.
- SQL-инъекции - получение несанкционированного доступа к информации с помощью особого языка запросов, требующего навыков программирования.
- Эксплойты нулевого дня - быстрое использование недостатков в системе безопасности после выхода ПО.
- Атаки методом полного перебора или брутфорс - взлом учетных записей путем перебора паролей с использованием специальных программ.
- DNS-туннелирование - превращение систем доменных имен в оружие хакеров путем использования протокола DNS для передачи трафика, не относящегося к этому протоколу.

В России ежегодно растут затраты государственных органов и госкомпаний на информационную безопасность. За 2020 затраты госсектора на обеспечение информационной безопасности составили 74,3 млрд. рублей (в 2019 году - около 66,4 млрд. рублей). А затраты только на реализацию федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика» в текущей редакции документа составляют 34,6 млрд руб. за период до 2024 г [2].

В 2022 году сфера безопасности перейдет к более широкому спектру продуктов и услуг, которые обеспечат защиту, повышение эффективности бизнеса, создадут дополнительную ценность для отдельных пользователей, компаний, общества государства. Анализ специалистов компании Hikvision позволил составить список ключевых трендов, которые существенно повлияют на индустрию безопасности в ближайшем будущем как всего мира в целом, так и России. Это такие тренды, как: искусственный интеллект везде и во всем; сочетание искусственного интеллекта и интернета вещей; конвергентные системы как замена традиционных хранилищ данных; облачные решения и услуги; высокая детализация изображения в любых условиях как новый стандарт отрасли; биометрические технологии для контроля доступа; использование модели Zero Trust: минимум доверия, максимум проверок; рост спроса на «зеленое» производство и «зеленые» технологии.

Таким образом, проблема кибербезопасности чрезвычайно важна в современных условиях для России. В основе успешной борьбы с киберпреступниками лежит развитие кадрового потенциала страны. Регулярное совершенствование знаний позволит своевременно выявлять попытки несанкционированного доступа к конфиденциальной информации, предотвращать взломы электронных баз данных, внедрения в бизнесс-процессы, что приведет к снижению финансовых потерь и технических, репутационных и иных рисков.

Источники и литература

1) Состав.ру: https://www.sostav.ru
2) CNews: https://www.cnews.ru
3) Connect: https://www.connect-wit.ru