Почуйко А. С. *Кибератаки – угроза безопасной бизнес-среде*
Научный руководитель: Макутонина Е. Ю., преп.

Новые информационные технологии улучшают качество жизни. Но внедрение современных информационных технологий, к сожалению, привело к появлению новых видов преступлений, таких как компьютерная преступность и компьютерный терроризм - незаконное вмешательство в работу электронно-вычислительных машин и компьютерных сетей, хищение, присвоение, вымогательство цифровой информации. Кибертерроризм - это новая форма терроризма, которая для достижения своих целей использует компьютеры и электронные сети, современные информационные технологии. Более того в настоящее время обеспечение информационной безопасности является одним из важнейших составляющих национальной безопасности государства. По своему механизму, способам сокрытия компьютерные преступления имеют определенную специфику, характеризуются высоким уровнем латентности и низким уровнем раскрываемости. Кибертерроризм становится серьезной проблемой, угрозой для мирового сообщества, опасность, которую он в себе несёт, справедливо сравнивают с ядерным, бактериологическим и химическим оружием.

Этапы киберпреступления. Целенаправленные нападения становятся все более изощрёнными, так как они включают различные этапы:

1) шпионаж;
2) проникновение;
3) распространение внутри имеющейся системы;
4) атака;
5) уничтожение следов киберпреступления[101].

Рассмотрим причины кибератак. Экономические мотивы киберпреступности. Принимая во внимание преступления, совершенные вне пределов Интернета, деньги являются основным мотивом для многих киберпреступников. Низкий уровень риска и большие финансовые вознаграждения побуждают многих киберпреступников заниматься разработкой вредоносных программных обеспечений, фишингом, кражей личных данных и мошенническими операциями с деньгами.

[101] NEC - Information Management. [Electronic resource] – Mode of access: http://www.nec.com/en/global/solutions/safety/info_management/cyberattack.html – Date of access: 17.02.2018.

Личные причины киберпреступности. Часто киберпреступниками являются люди, которые обижены кем-либо, и они хотят отомстить свои обидчикам или организациям, которые связаны с этим человеком.

Идеологические причины киберпреступности. Кибератаки совершаются по этическим, идеологическим или моральным причинам, с целью повреждения или отключения компьютерного оборудования и сетей с целью выражения недовольства в отношении отдельных лиц, корпораций, организаций или даже национальных органов власти.

Отсутствие знаний в области IT-технологий. Неспособность человека распознать несанкционированный доступ приводит к незаконному получению информации, что в свою очередь может привести к финансовым убыткам.

Основными угрозами кибертерроризма являются вредоносные программы, фишинг, кибератаки, направленные на кражу IP данных, финансовой информации, внутренние атаки.

Перейдём к последствиям кибертерроризма.

Причинение ущерба репутации. Доверие является важным элементом взаимоотношений с клиентами. Кибератаки могут нанести ущерб репутации Вашему бизнесу и подорвать доверие клиентов.

Это, в свою очередь, может привести к:

1) потере клиентов;
2) снижению продаж;
3) уменьшению прибыли.

Последствия подрыва репутации могут даже повлиять на отношения, которые вы можете иметь с партнёрами, инвесторами и другими третьими лицами, заинтересованными в Вашем бизнесе.

Угроза жизни. Угроза может быть даже для жизни: представьте себе злоумышленника, который может отключить системы жизнеобеспечения в больницах или получить контроль над беспилотными автомобилями.

Экономический ущерб. Кибератаки часто приводят к значительным финансовым потерям в результате:

1) кражи корпоративной информации;
2) кражи финансовой информации (например, банковские реквизиты или сведения о платёжной карте);

3) кражи денег;
4) перебоев в торговле (например, невозможность осуществлять онлайн сделки);
5) потери контрактов[102].

Как правило, организации, которые пострадали от кибератак также несут расходы, связанные с ремонтом пострадавших систем, сетей и оборудования.

На основе данных Аналитического Центра InfoWatch я провела исследование. В результате которого было выявлено, что чаще всего мишенью злоумышленников становятся организации финансового сектора (около 30%) и нефтегазовой отрасли (20%). Кроме того, объектами целенаправленных атак становятся данные банковских карт и счетов, персональные данные, сведения, составляющие коммерческую тайну, конфиденциальная информация и сведения, относящиеся к государственной тайне.

Проанализировав данные компании MacAfee, я сделала вывод, что последствия экономического ущерба от кибератак, наряду с незаконным оборотом наркотиков и пиратством, являются существенными. Однако следует учитывать, что оценки потерь об нанесённых кибертерроризмом ущербе, как правило, основываются на предположениях об их масштабах (так как зачастую потери трудно оценить).

Что касается мер противодействия кибертерроризму, то они включают в себя оценку текущей ситуации для выявления объектов, подлежащих защите, потенциальных угроз и масштабов причиненного ущерба.

Профилактические меры.Прежде всего предотвращение нападения лучше, чем обнаружение и устранение его. Такие меры должны включать:

1) ограничение прав доступа пользователей и времени работы в системе;
2) проверка защиты от вредоносных программ и вирусов;
3) внедрение программ, обнаруживающих аномалии;
4) использование IP-адресов и «белых списков» для предотвращения подключений к подозрительным сайтам.

Развитие людских ресурсов. Компании должны нанимать консультантов, имеющих опыт защиты от кибератак, которые проводят теоретический анализ, чтобы решить, как меры противодействия предпринять в будущем. Кроме того, сотрудники должны быть в курсе новейших информационных технологий.

[102] Alpha IT Labs - Cyber crime is the greatest threat to every company in the world. [Electronic resource] – Mode of access: https://alphaitlabs.com/ – Date of access: 22.02.2018.

Практические меры безопасности должны включать:

1) регулярное обновление и улучшение файрволлов;
2) обновление прошивки;
3) установка надёжных паролей;
4) изменение пароля Wi-Fi роутеров;
5) обращение к сотрудникам, которые используют собственную технику на рабочем месте, с просьбой установления антивирусных программ и включения файрволлов.

Всемирная Сеть является идеальной средой для террористической деятельности, поскольку доступ к ней крайне лёгок, в ней просто обеспечить анонимность пользователей, она никем не управляется и не контролируется. Кибертерроризм невероятно расширился из-за распространения Интернета. Кибертерроризм представляет собой социально опасную угрозу для человечества, причём степень этой угрозы в силу своей новизны не до конца еще осознана и изучена. Поэтому противодействие кибертерроризму должно стать одной из приоритетных задач в борьбе с преступностью. Международное сообщество должно разработать единые правила осуществления контроля за интернет информацией в целях предупреждения киберпреступлений.