Гуд А.Л

Жилинская Н.Н. . – к.э.н.,доцент

На сегодняшний день электронный бизнес обретает всё большую популярность в связи с существенным удобством. Правда многим компаниям часто приходится сталкиваться с угрозами вмешательства сторонних программ, хакеров. Это говорит о том что в любой системе защиты существует ряд аспектов, которые, не способны полностью устранить возможные риски, а так же предвидеть их. Безопасность имеет очень много рисков по сравнению с традиционными системами предпринимательства, поэтому для электронного бизнеса безопасность имеет большое значение. Клиенты, поставщики, сотрудники и многие другие люди используют какую-либо систему электронного бизнеса ежедневно. При этом данные участники отношений ждут соблюдения конфиденциальности информации, предоставляемой ими. Хакеры являются одной из главных угроз в интернет бизнесе. Некоторые вопросы безопасности включают в себя ведение информации о клиентах частного и конфиденциального характера, их достоверности и целостности.[4]

Как правило, существует два типа угроз: внутренние и внешние вторжения в систему. Защита от внутренних угроз проводится по техническим и внутренним аспектам:

1) Техническая сторона безопасности (подразумевает поддержку паролей и их периодические изменения, предоставления минимум прав при администрировании системы)[2]

2) Организационный аспект безопасности (основывается на тестировании системы на предмет хакерства и введении процедур распознавания атак со стороны хакеров)[2].

Основные области информационной безопасности электронного бизнеса:

- Администрирование;
- Контроль доступа;
- Контроль за потенциально опасным содержимым;
- Определение атак;
- Защиту корпоративного примера;
- Определение событий безопасности;
- Право на частную, персональную информацию;
- Аутентификацию (механизм объективного подтверждения информации).

Для электронного бизнеса применяются различные методы и средства защиты информации:

a) Защищенные коммуникационные протоколы;
b) Механизм аутентификации и авторизации;
c) Средства контроля доступа к рабочим местам сети;
d) Антивирусные комплексы;
e) Программы обнаружения атак.

Точное применение методов защиты позволяет построить эффективную и надежную систему обеспечения информационной безопасности. Учитывая что основная проблема безопасности электронного бизнеса не соблюдение основных факторов безопасности, как технических так организационных, которые в свою очередь должны быть тесно связаны, обеспечивая целостность и гибкость защищенных проектов электронного бизнеса. Безопасность от внешних вторжений обеспечивается различными программными фильтрами, которые распознают и предотвращают попытки хакерства на начальных этапах. Наиболее распространенные фильтры угроз представляются в виде различных маршрутизаторов, брандмауэров, шлюзов приложений, систем отслеживания вторжений, средств оценок защищенности. Однако существует проблема не позволяющая обезопасить информационную базу от угроз наверняка. Это обусловлено постоянным развитием технологий, которые законодательная база не может своевременно предусмотреть. Поэтому зачастую поймать злоумышленника бывает крайне сложно, а потеря корпоративных данных может нанести существенный урон всей деятельности предприятия, соответственно можно предположить что основная задача повышения качества безопасности, лежит в том что бы вовремя обновлять и дорабатывать методы её защиты от современных вредоносных программ, учитывая что методы безопасности, как и методы взлома развиваются в одинаковом темпе.[4]

Список используемых источников:

1. Беляцкая Т.Н. Электронная экономика: генезис и развитие – Saarbruecken (Germany): LAP LAMBERT Academic Publishing, 2014

2. Сергей Знаменский – технический консультант компании HP Russia & CIS (Москва): [Электронный ресурс]. - https://www.osp.ru/os/2001/05-06/180177

3. Петренко, С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.С. Симонов.– М.: Компания АйТи; ДМК Пресс, 2004.

4. Онлайн банк, все о интернет банках, [Электронный ресурс] - http://credit-vbanke.ru

НЕЗАЩИЩЕННОСТЬ КЛИЕНТОВ ПРИ РАБОТЕ С СЕРВИСАМИ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Масюк Л.С., Михаленок Н.А.

Ермакова Е.В. – к.э.н., доцент каф. менеджмента

Одним из видов электронного бизнеса считается электронная коммерция. В соответствии с документами ООН, бизнес признается электронным, если хотя бы две его составляющие из четырех (производство товара или услуги, маркетинг, доставка и расчеты) осуществляются с помощью Интернета. Поэтому в такой интерпретации обычно полагают, что покупка относится к электронной коммерции, если, как минимум, маркетинг и расчеты производятся средствами Интернета. Более узкая трактовка понятия "электронная коммерция" характеризует системы безналичных расчетов на основе пластиковых карт. Поэтому ключевым вопросом для внедрения электронной коммерции является безопасность. [1]

Безопасность — это состояние, при котором отсутствует возможность причинения ущерба потребностям и интересам субъектов отношений. Применительно к электронной коммерции определение безопасности можно сформулировать как состояние защищенности интересов субъектов отношений, совершающих коммерческие операции с помощью технологий электронной коммерции, от угроз материальных и иных потерь.

Обеспечение информационной безопасности является одним из ключевых моментов обеспечения безопасности организаций. Как считают западные специалисты, утечка 20 % коммерческой информации в шестидесяти случаях из ста приводит к банкротству предприятия. Потому физическая, экономическая и информационная безопасность взаимосвязаны.[2]

Электронная коммерция подвержена рискам в той же степени, что и коммерция в ее традиционном понимании. Наряду с «классическими» присутствуют и новые, до этого момента неизвестные риски, управление которыми является сложной задачей в силу их неполной изученности.

Приведем классификацию возможных типов мошенничества в электронной коммерции:

- транзакции (операции безналичных расчетов), выполненные мошенниками с использованием правильных реквизитов карточки (номер карточки, срок ее действия и т.п.);
- получение данных о клиенте через взлом БД торговых предприятий или путем перехвата сообщений покупателя, содержащих его персональные данные;
- магазины-бабочки, возникающие, как правило, на непродолжительное время, для того, чтобы исчезнуть после получения от покупателей средств за несуществующие услуги или товары;
- увеличение стоимости товара по отношению к предлагавшейся покупателю цене или повтор списаний со счета клиента;
- магазины или торговые агенты, предназначенные для сбора информации о реквизитах карт и других персональных данных покупателя.

Основным риском для интернет-магазинов является риск утечки конфиденциальных данных, в том числе – персональных данных клиентов. Исходя из статистических данных можно наблюдать, что из года в год объем похищенных персональный данных растет. Если в 2013 году это цифра составляла 500 миллионов записей по всему миру, то на 2015 это значение увеличилось до 1,2 миллиардов записей. Основным поводом для беспокойства в сфере онлайн безопасности является кража личных данных, такого мнения придерживаются 63% пользователей. Второе место отводится мошенничеству с кредитными картами, данным видом угрозы обеспокоены 45% интернет-пользователей. [3]

Если говорить о компаниях, опасности и потенциальные киберпреступления намного превосходят их готовность противодействовать атакам. Порядка 63% компаний не имеют никаких процедур или планов действий на случай их возникновения. Опрос организаций на наличие систем безопасности показал, что такие системы применяют 37% организаций, 12% имеют системы, но не используют ее. Что касается остальных организаций, составляющие 51% из общего числа, у них отсутствует система мероприятий по борьбе с кибератаками. В итоге получаем, что, сотрудничая с какой-либо организацией, шанс быть защищенными при кибератаке составляет около 50%.[3]

Существует множество причин, по которым не удается защитить данные в сети. В качестве респондентов для опроса выступали IT-специалисты, 93% из которых сообщили о существующих проблемах в сфере защиты информации.

Особое внимание стоит уделить такому виду угрозы, как уязвимость нулевого дня. Уязвимость нулевого дня – уязвимость в программном обеспечении или оборудовании, о которой не знает производитель. До того как производитель узнает об уязвимости и внесет исправления, злоумышленник может воспользоваться ею для достижения своих целей. Уязвимости нулевого дня влекут за собой появление новых способов распространения вредоносного кода, что активно используется киберпреступниками для создания эффективного механизма заражения. Опасность из-за уязвимости нулевого дня выросла на 125% с 2013 года. В этом случае хакеры обнаруживают уязвимость, запускают атаку и завершают ее в тот же день, так что у систем безопасности нет времени отреагировать.

Отдельным риском считается хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Это уже не нарушение работоспособности сервиса или конфиденциальности данных. Это довольно сложные, в том числе и оффлайновые операции, по извлечению выгоды с помощью манипуляций с данными и процессами интернет-магазина.

В последнее время получил распространение фишинг. Как можно догадаться, «рыбкой» в данном случае является жертва, а точнее — ее персональные данные о банковском счете. Методов фишинга несколько, но в основном пользователю приходит письмо на фирменном бланке, в котором предлагается отправить свои персональные данные якобы «для перерегистрации» или «обновления базы данных», либо прямым ответом, либо после перехода по ссылке на сайт финансового учреждения. Во втором случае пользователя направляют не на реальный сайт, а на поддельный, на самом деле принадлежащий мошенникам.

Рассматривая ситуацию в Республике Беларусь, необходимо отметить стабильность в количестве совершенных преступлений в сфере Интернет. Так в 2016 году в сравнении с 2015 годом число выявленных преступлений в сфере высоких технологий увеличилось на 1,3% (с 2 440 до 2 471), в том числе по областям: Брестская – 260 (276), Витебская – 286 (243), Гомельская – 353 (354), Гродненская – 206 (249), Минск – 818 (776), Минская – 311 (304), Могилевская – 237 (238).[4]

Непрерывное развитие сетевых технологий при отсутствии постоянного анализа безопасности приводит к тому, что с течением времени защищенность сети падает. Появляются новые неучтенные угрозы и уязвимости системы. Решением данной проблемы для организаций электронной коммерции может быть адаптивная безопасность сети. Она позволяет обеспечивать защиту в реальном режиме времени, адаптируясь к постоянным изменениям в информационной инфраструктуре.

Электронная торговля как новая форма мирового рыночного хозяйства повышает эффективность экономики, а также формирует условия для ускорения промышленного роста. В процессе развития электронная торговля будет сталкиваться с новыми проблемами, в том числе проблемами информационной безопасности. Системы защиты электронной коммерции должны эффективно работать на всех уровнях, а поэтому проблеме обеспечения информационной безопасности следует уделить особое внимание, заключающееся в выборе необходимых средств защиты ещё на этапе проектирования информационных систем электронных торговых площадок.[5]

Список использованных источников:

1. http://mirznanii.com/a/310885/vozmozhnosti-organizatsii-biznesa-i-kommertsii-v-internet
2. http://center-yf.ru/data/stat/Bezopasnost-elektronnoi-kommercii.php
3. https://ru.vpnmentor.com/blog/статистика-по-использованию-vpn-и-защите/
4. http://mvd.gov.by/main.aspx?guid=381973
5. http://moluch.ru/conf/tech/archive/126/8481/