**Информация о вопросах профилактики преступлений, совершаемых с использованием возможностей глобальной компьютерной сети Интернет.**

В современном мире наблюдается активное развитие, внедрение и совершенствование электронных информационных систем, автоматизация множества процессов.

В условиях развития цифровой экономики информационный ресурс стал одним из наиболее мощных рычагов экономического развития. Своевременное владение актуальной информацией - залог успеха в любом виде хозяйственной деятельности.

При этом наряду со стремительным развитием компьютерных технологий обострилась проблема защиты информации, несанкционированный доступ к которой может привести к причинению материального вреда и иным негативным последствиям.

Следует отметить, что развитие современных информационных и компьютерных технологий всегда отражается практически на всех сферах жизнедеятельности общества, а их повсеместное использование приводит не только к повышению уровня жизни общества, но и к росту числа совершаемых преступлений в сфере компьютерной информации.

В настоящее время проблемы, связанные с противодействием киберпреступности, являются чрезвычайно важными на государственном уровне. Все чаще под ударами кибератак оказываются различные предприятия и организации, как государственной, так и частной формы собственности.

Одной из актуальных проблем на сегодняшний день остается хищение денежных средств субъектов хозяйствования путем несанкционированного доступа к системам дистанционного банковского обслуживания, электронным почтовым ящикам, а также путем заражения компьютеров вредоносным (шпионским) программным обеспечением.

Справочно: в столице ежемесячно фиксируется не менее 3 таких преступлений.

Несанкционированный доступ к компьютерной информации, позволяющий совершать хищения денежные средств, в том числе виртуальных, может осуществляться посредством таких способов, как «фишинг» и «фарминг».

Фишинг представляет собой способ несанкционированного доступа к конфиденциальным данным пользователя посредством Интернет-писем или СМС-рассылки, содержащих адрес активной ссылки на подставной сайт-близнец, или загрузки вредоносного программного обеспечения.

Фарминг один из самых прогрессирующих и опасных видов «фишинга», базируется на процедуре внедрения вредоносного кода на персональный компьютер пользователя или сервер, который автоматически производит замену оригинального ip-адреса на поддельный.

В основе указанных методов лежит обман пользователя в целях завладения логинами и паролями для доступа к аккаунтам различных Интернет-сервисов, а также открытыми и приватными ключами, кодовыми словами для входа в электронные почтовые ящики и криптокошельки.

Механизм работы «фишинга» включает 2 основных способа доступа к конфиденциальным данным: собственноручный ввод данных на поддельных сайтах или загрузка вредоносной программы. Указанные способы реализуются посредством спам-рассылки писем преимущественно через электронную почту. В них содержаться указания, необходимые для выполнения под угрозой негативных последствий (штрафные санкции и т.д.).

Такие письма содержат ссылку, ведут на ресурс, где необходимо ввести личные данные, либо включает в себя автоматическую загрузку вредоносного программного обеспечения, которое, помимо прочего, может быть внедрено во вложение к письму (pdf- или иные файлы). Попадая на устройство, вирусная программа осуществляет заложенные в ней функции (считывает вводимые либо уже сохраненные данные на компьютере).

Справочно: к примеру, в июле текущего года на сайте электронного правительства Казахстана обнаружили документ, зараженный вредоносным программным обеспечением, основной задачей которого являлось извлечение учетных данных и постепенный захват контроля над устройством.

В свою очередь, «фарминг» представляет собой достаточно сложный механизм, суть которого заключается в подмене Интернет-страницы на созданную злоумышленником копию за счет взлома сервера.

Владельцами данных сайтов являются крупные организации и предприятия, обеспечивающие безопасность своих страниц. Порой злоумышленникам удается обойти защиту и получить доступ к конфиденциальной информации как самой организации, так и ее клиентов.

Справочно: проведенные исследования банковских учреждений Российской Федерации компанией «Positive Technologies» (один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений) показали, что 75% банков уязвимы к атакам методами социальной инженерии, в 58% банков выявлены недостатки управления учетными записями и паролям. Кроме того, в 58% банков получен доступ к банковским системам.

Проведенный в УСК по г. Минску анализ показал, что для г. Минска, как и в целом для Республики Беларусь, наиболее характерен такой метод хищения денежных средств субъектов хозяйствования как «фишинг».

Обнаружить попытку фишинговой атаки не сложно, если обладать базовой компьютерной грамотностью и уделять должное внимание анализу и проверке писем, посещаемых сайтов и веб-страниц. Необходимо обращать внимание на URL-адрес ресурса, поскольку при фишинге адрес сайта отличается на 1-2 буквы, цифры или 1-2 символа. Получая электронные письма, следует проанализировать не только содержимое, но и имя отправителя.

Справочно: согласно аналитическим данным по киберпреступности более 70 % организаций (предприятий) в мире не готовы к нарушениям безопасности, а пользователи глобальной компьютерной сети Интернет открывают каждое 3 фишинговое письмо. В среднем в мире компании (организации) требуется более 6 месяцев, чтобы установить факт утечки данных. Более 50% кибератак вовсе не обнаруживается.

Обычно письма содержат призывы к активным действиям пользователя (представить адресату конфиденциальные данные, произвести оплату за товар, услуги, в том числе на новый расчетный счет).

На сегодняшний день лучшими методами защиты является шифрование, антивирус, брандмаузер, цифровые подписи, двухфакторная аутентификация и использование различного программного обеспечения, которое способно в автоматическом режиме сканировать систему на наличие уже активированных вирусов и попыток внедрения новых вредоносных программ.

Таким образом, повышенная угроза и степень распространения вышеуказанных атак побуждают к принятию активных действий по формированию мер предупреждающего характера. Первым шагом к улучшению киберзащиты является понимание того, насколько организация (предприятие) подвержена риску атак, и определение уязвимостей, которые должны быть устранены.

На основании вышеизложенного, руководствуясь статьей 4 Закона Республики Беларусь от 13.07.2012 № 403-3 «О Следственном комитете Республики Беларусь», в целях противодействия киберпреступности и повышения уровня кибербезопасности прошу:

рассмотреть настоящее информационное письмо с руководителями структурных подразделений с целью недопущения совершения преступлений в сфере высоких технологий;

на системной основе информировать сотрудников о проявлении  
осторожности и бдительности, соблюдении правил безопасности при  
работе в глобальной компьютерной сети Интернет;

с учетом темпа развития информационных систем, внедрения новых цифровых технологий, случаев хищения денежных средств со счетов организаций (предприятий), рекомендовать сотрудникам принимать дополнительные меры по осуществлению безопасности при работе в глобальной компьютерной сети Интернет, предупредить

о недопустимости игнорирования и пренебрежения требований, направленных на сохранение благосостояния организаций (предприятий);

обеспечить наличие в штате специалистов по информационной безопасности в целях сохранения личных данных клиентов и сотрудников организаций (предприятий), предупреждения фактов хищения денежных средств и иных негативных последствий.

Также необходимо понимать, что злоумышленник не сможет достичь своей цели и похитить денежные средства, если атака будет вовремя выявлена и остановлена, а это возможно на любом ее этапе, при своевременном принятии соответствующих мер защиты. Необходимо проверять почтовые вложения в изолированном окружении, не полагаясь исключительно на антивирусные решения, установленные на рабочих станциях пользователей. Крайне важно своевременно получать уведомления систем защиты и незамедлительно реагировать на них. Для этого необходим постоянный мониторинг событий безопасности силами внутреннего или внешнего подразделения оперативного центра безопасности.

В целях эффективного противодействия активно развивающейся киберпреступности важно не скрывать произошедшие инциденты, а участвовать в обмене информацией об атаках, незамедлительно сообщать о них в правоохранительные органы.